

Technical Report 1340

Determining the Requisite Components of Visual Threat Detection to Improve Operational Performance

Laura Zimmerman and Shane Mueller

Applied Research Associates

Jeff Grover

Dynamics Research Corporation

Christopher L. Vowels

U. S. Army Research Institute

April 2014



**United States Army Research Institute
for the Behavioral and Social Sciences**

Approved for public release; distribution is unlimited.

**Army Research Institute
for the Behavioral and Social Sciences**

**Department of the Army
Deputy Chief of Staff, G1**

Authorized and approved for distribution:

**MICHELLE SAMS, Ph.D.
Director**

Research accomplished under contract
for the Department of the Army by:

Applied Research Associates
Dynamics Research Corporation

Technical Review by:

Jennifer Murphy, U.S. Army Research Institute
Steven F. Burnett, U.S. Army Research Institute

NOTICES

DISTRIBUTION: Primary distribution of this Technical Report has been made by ARI. Address correspondence concerning this report to U.S. Army Research Institute for the Behavioral and Social Sciences, ATTN: DAPE-ARI-ZXM, 6000 6th Street (Bldg. 1464 / Mail Stop: 5610), Ft. Belvoir, Virginia 22060-5610.

FINAL DISPOSITION: Destroy this Technical Report when it is no longer needed. Do not return it to the U.S. Army Research Institute for the Behavioral and Social Sciences.

NOTE: The findings in this Technical Report are not to be construed as an official Department of the Army position, unless so designated by other authorized documents.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
1. REPORT DATE (DD-MM-YYYY) April 2014		2. REPORT TYPE Final		3. DATES COVERED (From - To) May 2009 – June 2011	
4. TITLE AND SUBTITLE Determining the Requisite Components of Visual Threat Detection to Improve Operational Performance				5a. CONTRACT NUMBER W74V8H-04-D-0048	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER 622785	
6. AUTHOR(S) Laura Zimmerman, Shane Mueller; Jeff Grover; Christopher L. Vowels				5d. PROJECT NUMBER A790	
				5e. TASK NUMBER 370	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Applied Research Associates Dynamics Research Corp. 1750 Commerce Blvd. 60 Frontage Road Fairborn, OH 45324-6362 Andover, MA 01810				8. PERFORMING ORGANIZATION REPORT	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) U. S. Army Research Institute for the Behavioral & Social Sciences 6000 6 th Street (Building 1464 / Mail Stop 5610) Fort Belvoir, VA 22060-5610				10. SPONSOR/MONITOR'S ACRONYM(S) ARI	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) Technical Report 1340	
12. DISTRIBUTION/AVAILABILITY STATEMENT: Distribution Statement A: Approved for public release; distribution is unlimited.					
13. SUPPLEMENTARY NOTES Contracting Officer's Representative: Dr. Christopher L. Vowels					
14. ABSTRACT This report describes research initiated to understand the requisite components of visual threat detection for the operational environment and to assess the critical behaviors Soldiers rely on to proficiently detect threats. To understand the process of visual threat detection, a focused literature review of military doctrine and academic sources was completed, in-depth interviews were conducted with Soldiers who had recent deployment experiences, and computer-controlled exercises were used to investigate the primary processes of threat detection. Those processes include dynamic threat monitoring, threat prioritization, and causal reasoning. Based on findings from that research, a model of visual threat detection was created. The findings are summarized in two reports. This report presents evidence that suggests visual threat detection is a cyclical process requiring numerous, concurrent perceptual and cognitive processes, and may be enhanced by focusing training development on the principle components such as causal reasoning. The second report will discuss the development and evaluation of a research-based training exemplar. Visual threat detection pervades many military contexts, but is also relevant in similar settings such as law enforcement and airport security; therefore, this research has the potential to inform a wider audience.					
15. SUBJECT TERMS Threat detection, Reasoning, Irregular warfare, Attention, Memory, Improvised explosive devices					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified	Unlimited Unclassified	98	Cindy Underwood
					19b. TELEPHONE NUMBER 254-288-3801

Standard Form 298 (Rev. 8-98)

Technical Report 1340

**Determining the Requisite Components of Visual
Threat Detection to Improve Operational Performance**

Laura Zimmerman and Shane Mueller

Applied Research Associates

Jeff Grover

Dynamics Research Corporation

Christopher L. Vowels

U. S. Army Research Institute

Fort Hood Research Unit

Brian T. Crabb, Chief

U.S. Army Research Institute for the Behavioral and Social Sciences

6000 6th Street , Building 1464

Fort Belvoir, VA 22060

April 2014

Approved for public release; distribution is unlimited

ACKNOWLEDGEMENTS

We offer our sincere thanks to the Soldiers who have provided insights and participated in the research on the present topic. Their efforts continue to assist in our understanding of the operational environment.

DETERMINING THE REQUISITE COMPONENTS OF VISUAL THREAT DETECTION TO IMPROVE OPERATIONAL PERFORMANCE

EXECUTIVE SUMMARY

Research Requirement:

The Army operates in a variety of geographical and cultural settings. The Army mission has evolved with the environments Soldiers are operating in and Soldiers, likewise, have adapted their knowledge and skills to complete the necessary missions in those diverse settings. A necessary part of most missions in the operational environment is the ability to visually detect potential threats, regardless of the characteristics of that environment. This research provides a contemporary perspective of visual threat detection to enhance pre-deployment training in order to prepare Soldiers for missions where detecting threats is imperative.

Procedure:

Military doctrine and academic sources were reviewed to gather and assess the primary topics and issues for visual threat detection. Likewise, Soldiers with recent deployment experience were interviewed to collect their knowledge and understanding of how to detect potential threats in operational settings. Those results provided the impetus for developing computer-controlled exercises to study the primary components of visual threat detection. Similarly, civilian law enforcement officers were observed while on duty in order to provide a secondary context to check the concepts provided by Soldiers. These naturalistic observations provided a real-time look at the application of visual threat detection skills.

Findings:

The review and analysis of the literature, interviews with Soldiers, and results from the computer-controlled exercises, indicate that visual threat detection is a cyclical process involving many concurrent perceptual and cognitive processes. The current results suggest the primary components of visual threat detection are:

- *dynamic threat monitoring* or maintaining a vigilant search of the environment among competing visual cues,
- *threat prioritization* or identifying high priority threats versus low priority threats, and
- *causal reasoning* or deliberately engaging in a reasoning process in order to determine why potential threat cues are present.

To study visual threat detection accurately, a combination of methods and metrics is required. For instance, results from research using vigilant search tasks have provided insight into lower level perceptual processes, while measures involving causal reasoning have provided information on higher-level cognitive processes. Based on that previous research, a model of visual threat detection was developed that combines perceptual decision-making and vigilance.

Utilization and Dissemination of Findings:

By identifying the critical components of the threat detection process, the present findings provide guidance about how to enhance training for Soldiers who are routinely required to perform mounted and dismounted patrols and for Soldiers performing related operations such as route clearance. The findings could also be extended to other professions where rapid and accurate interpretations of the visual environment are necessary, including law enforcement and airport security.

DETERMINING THE REQUISITE COMPONENTS OF VISUAL THREAT DETECTION TO IMPROVE OPERATIONAL PERFORMANCE

CONTENTS

	Page
INTRODUCTION	1
Goals and Approach.....	3
SUMMARY OF LITERATURE REVIEW FINDINGS	4
DECISION MODELS	5
EXPERT MENTAL MODEL DEVELOPMENT	8
The Threat Detection Loop.....	8
PHASE I: BACKGROUND INVESTIGATIONS	10
Method	11
Phase Ia: Preliminary data collection.....	11
Participants.....	11
Materials	11
Procedure	12
Analysis.....	12
Phase Ia: Results and discussion.....	13
Threat questionnaire.....	13
Interviews.....	14
Phase Ib: Expertise capture from analogous domain – Baltimore, MD police department.....	14
Participants.....	16
Procedure	16
Phase 1b: Results and discussion.....	16
Relevance to military patrol activities	17
Discussion: Background investigations	17
PHASE II: PILOT TEST	18
Method	18

CONTENTS (Continued)

	Page
Phase II: Data collection	18
Participants.....	18
Materials	19
Procedure	19
Analysis.....	20
Phase II: Results and Discussion	21
Threat questionnaire.....	21
Combined analysis: Phases I and II	23
Imagery Analysis	25
Plan for Testing the Model of Expert Threat Detection	29
PHASE III: PRELIMINARY EXPERIMENT	34
Phase III: Interview Results	34
FUTURE RESEARCH	38
SUMMARY AND CONCLUSIONS	39
REFERENCES	41

APPENDICES

APPENDIX A. ACRONYMS	A-1
APPENDIX B. DEMOGRAPHIC QUESTIONNAIRE	B-1
APPENDIX C. THREAT QUESTIONNAIRE	C-1
APPENDIX D. INTERVIEW PROTOCOL – PHASE I (1A) SESSION 1 AND 2 (ENLISTED).....	D-1
APPENDIX E. SHORT-ANSWER PROTOCOL – PHASE I (1A) SESSION 2 (OFFICERS)	E-1
APPENDIX F. SUMMARY OF RIDE-ALONG ACTIVITIES – PHASE I (1B).....	F-1
APPENDIX G. IMAGES FOR IMAGERY ANALYSIS – PHASE II.....	G-1
APPENDIX H. INTERVIEW PROTOCOL – PHASE II	H-1
APPENDIX I. SCREEN CAPTURE OF IMAGERY ANALYSIS EXERCISE PHASE II	I-1
APPENDIX J. EXAMPLE ANNOTATIONS FROM IMAGERY ANALYSIS EXERCISE PHASE II	J-1

	Page
APPENDIX K. IMAGERY ANALYSIS WORD LIST – PHASE II	K-1
APPENDIX L. MAJOR COMMENTS FROM INTERVIEWS – PHASE II	L-1
APPENDIX M. EXERCISE DESCRIPTIONS – PHASE III	M-1
APPENDIX N. INTERVIEW PHOTOS – PHASE III	N-1

TABLES

TABLE 1. HIGHEST MEAN RATINGS PER THREAT QUESTIONNAIRE CATEGORY BY GROUPS IN PHASE I.....	15
TABLE 2. “RIDE-ALONG” SCHEDULE.....	16
TABLE 3. HIGHEST MEAN RATINGS PER THREAT QUESTIONNAIRE CATEGORY BY GROUPS IN PHASE II.....	22
TABLE 4. HIGHEST MEAN RATINGS PER THREAT QUESTIONNAIRE CATEGORY BY GROUPS IN PHASES I AND II	24
TABLE 5. CROSS-TABULATION OF LIKELIHOOD AND SEVERITY RATINGS ACROSS ALL IMAGES	26
TABLE 6. INTERVIEW DATA CATEGORIES	28
TABLE 7. METRICS FOR ASSESSING BEHAVIORS ASSOCIATED WITH EXPERTISE IN THE THREAT DETECTION LOOP.....	33

FIGURES

FIGURE 1. THE OODA LOOP	6
FIGURE 2. THREE LEVELS OF PROCESSING IN THE RECOGNITION-PRIMED DECISION MODEL.....	7
FIGURE 3. DIAGRAM OF THE THREAT DETECTION LOOP	8
FIGURE 4. IMAGERY ANALYSIS EXERCISE SCREEN SHOT.....	20
FIGURE 5. ANNOTATION EXAMPLE.....	25
FIGURE 6. THE INFLUENCE OF EXPERIENCE, KNOWLEDGE, AND EXPERTISE ON THREAT DETECTION PROCESSES	
FIGURE 7. MEASURABLE BEHAVIORS OF EXPERTS IN THE THREAT DETECTION LOOP.....	32

DETERMINING THE REQUISITE COMPONENTS OF VISUAL THREAT DETECTION TO IMPROVE OPERATIONAL PERFORMANCE

Introduction

Field Manual (FM) 3-24, *Counterinsurgency*, describes the nature of the operational environment (OE)¹ as extremely uncertain, primarily because insurgents use diverse mechanisms to exploit a variety of threats, such as different types of Improvised Explosive Devices (IED), snipers, and simple and complex attacks. Field Manual 3-24 further emphasizes how critical it is for Soldiers and leaders on the ground to conduct analysis of the OE. That analysis leads to a better understanding of both animate (persons) and inanimate threats (IEDs). The IEDs, which are only one of many existing threats in current OEs, can take many forms and can be concealed in various locations throughout the areas of operations (AO). As discussed in FM 7-0, *Training Units and Developing Leaders for Full Spectrum Operations*, the Army has shifted its training focus from tactics intended to overcome Cold War enemies to tactics that prepare Soldiers for fighting in hybrid warfare environments to defeat the variety of threats embedded within those environments. For instance, one of the major pillars in FM 3-90.119, *Combined Arms Improvised Explosive Device Defeat Operations*, is to train proactive skills for IED defeat. One of those skills is to conduct different levels of search operations, with “basic search”² being a level that all Soldiers must be able to execute. As part of basic search, Soldiers must conduct searches of people, vehicles, areas, and buildings to assist in determining the appropriate level of risk.

As noted in Vowels (2010), the large amount of sensory input, distracters, and information in the OE makes threat detection a seemingly impossible task. Enemies continue to employ numerous types of threats, while continuously improving their threat concealment tactics. Soldiers are shifting their focus to a more proactive threat search and response strategy based on the transition of military leaders’ focus on understanding and training for irregular warfare coupled with knowledge gained from Soldiers’ Observations, Insights, and Lessons (OIL). However, this new focus does not fully address the required changes in cognition that would allow Soldiers to perceive, process, and interpret threats in irregular environments. Soldiers, as all humans are, are susceptible to bias and misperceptions, especially in terms of predicting future states of the world. Taleb’s (2007) overview, for instance, recounts that we are prone to think our interpretation of the world is how the world actually exists; however, our interpretations can often be misleading. This is an important lesson for Soldiers operating in an irregular environment where the difference between guessing, based on presumptions, and predicting, based on reliable information, can have disastrous consequences. Environments ruled by uncertainty exacerbate errors in perception and reasoning (Lopes, 1982; see also Ayton, Hunt, & Wright, 1989). Making predictions allows Soldiers to move into a controlling and preventative stance and away from the reactive posture that results from guessing. However, as Taleb forewarns, using the past to predict the future can often be an inaccurate strategy, particularly in dynamic and uncertain decision environments.

¹ Appendix A contains a list of the acronyms used in this report.

² See pgs. 5-12, sections 5-39 through 5-41 in FM 3-90.119 for further description.

Operational settings have always been inherently uncertain, forcing Soldiers to accomplish their mission in areas full of noise and missing information. The natural biases (Tolcott, Marvin, & Bresnick, 1996) that humans rely on can degrade the ability to accurately interpret these uncertain environments. This seems even truer in today's OE, where adversaries employ a wide range of weapons and often shift their tactics, techniques, and procedures (TTP) making it difficult to track and adjust operations to their movement. The random nature within the OE is analogous to the noise inherent in capital markets.

Capital markets³ are comprised of thousands of random variables (e.g., company solvency issues, potential stock splits). Investors typically take a broad sample of the market in order to capture this variance and make investment decisions. Unfortunately, the odds of making successful decisions tend not to increase above chance level. Similarly, a number of random variables determine the irregular nature of the OE (e.g., al-Qa'ida influence on a village, tit-for-tat retaliation, new enemy TTP). Based on findings from the capital market literature, it is hypothesized that if a randomly selected Soldier selects any one or more OE random variables to guide his/her decisions about a threat, on average, s/he will not be able to make a predictive decision greater than chance. If the Soldier possesses some type of insider information, and can make use of it, predictive ability may increase above chance. Nevertheless, information about the OE fluctuates unpredictably, making the forecasting of enemy intentions and actions quite difficult. In this research, we examined how Soldiers perceive and interpret the visual environment as a means of understanding how Soldiers operate in and make above-chance predictions in an uncertain decision environment.

The Army understands the importance of enhancing the innate skills and attributes of Soldiers, but focus has largely been on developing technology to assist in improving threat detection. While beneficial, assets like unmanned aerial vehicles (UAV) do not detect all threats nor can they reason about potential threat. Humans, who can perceive, process, and reason about indicators, actions, and conditions in the environment are still the most effective threat detectors. When technologies fail or are not available, the human visual system and decision-making ability are the requisite pieces of equipment Soldiers will bring with them on each mission. Soldiers must be able to vigilantly search the visual environment for indicators of threat and do so among competing visual cues. They must also prioritize which (potential) threats are most important for a given situation. As Soldiers develop higher-level threat detection skills, they also determine why certain cues are present and how those cues change the global meaning of a situation from non-threatening to threatening. Ultimately, enhancement of these skills provides Soldiers with a predictive interpretation (versus a reactive understanding) of the OE.

This report addresses the challenge of developing a perceptual and cognitive model that accurately sifts information and noise from a random environment to allow the observer to detect indicators that are predictive of threat. Within that model, experience and/or focused training should affect cyclical information processing mechanisms and allow improved detection of visual threats, greater than chance. Particularly, the model will demonstrate the primary skills of visual threat detection in relation to experience and training and take into account that perceptual and cognitive resources are finite.

³ For a focused theoretical discussion of market theory, refer to research on the Efficient Market Hypothesis (Fama, 1970) and Modern Portfolio Theory (Markowitz, 1952).

Goals and Approach

Given the need of the Army to shift its focus to combat adaptive enemies on a visually dynamic and irregular battlefield, research was initiated to better understand and, ultimately, enhance Soldiers' visual threat detection performance in operational settings. The overarching research goal was to combine information from military doctrine and knowledge from Soldiers based on recent deployment experiences with tenets of current psychological theory to improve understanding and application of threat detection in irregular environments. Embedded within the research goal are several objectives, including gaining a better understanding of how the Army trains attention and threat detection, identifying mechanisms, and creating training exemplars likely to enable superior threat detection performance.

A crucial goal of this research was to provide a research-based training exemplar that could reduce errors as well as increase speed, flexibility, robustness, and (potentially) skill retention of visual threat detection used by Soldiers. For instance, as discussed in *Phase II: Pilot Test*, investigating processes such as dynamic threat monitoring/search, threat prioritization, and causal reasoning directly informed development of the training exemplar. Information gathered from Soldiers at various proficiency levels provided data used to examine the influence of experience on these processes. One primary goal of this research was to develop a training approach for deploying Soldiers that focused on the primary cognitive processes of visual threat detection that proficient performers rely on. The development of the training exemplar is discussed in a complementary report (Zimmerman, Mueller, Daniels, & Vowels, In Preparation).

To create appropriate research materials, Soldiers who had recent operational experience completed a series of exercises in order to identify the skills Soldiers rely on during visual threat detection exercises. Based on skill identification, threat detection exercises, and methods requisite in the OE were identified and prioritized. By identifying the most important processes, experimentation plans, and resources were developed to best accomplish the three objectives of this research. The first objective entailed identification and prioritization of the key threat cues and indicators present in the OE. The second was to develop performance measures that would allow for an assessment of Soldiers' threat detection performance, thereby enabling an identification of more proficient performers. The third objective was to test a model developed from the analysis of proficient performers that describes 'expert' threat detection.

The following report presents findings from three preliminary research phases that will form the basis of further experimentation and training exemplar development and evaluation. Initially, a summary of findings is provided from a preliminary literature review (Zimmerman, Mueller, & Grover, 2009). Then, the three phases of research are discussed. Phase I consists of the research conducted to gain an initial understanding of how threat detection occurs in the OE. Soldiers participated in interviews and provided responses to questionnaires (Phase 1a). In support of Phase I, police officers on patrol were observed (Phase 1b). Phase II, consisted of an imagery analysis exercise, questionnaires, and in-depth interviews. This phase concluded with refinement of the research materials and that supported the testing of a threat detection model. Phase III focused on an assessment of those refined materials. The materials included dynamic threat monitoring/search, threat prioritization, and causal reasoning exercises. Soldiers also

provided feedback about the accuracy and relevance of those materials. The final section of the report is a summary of the findings.

Summary of Literature Review Findings⁴

There is a large collection of scientific research demonstrating the influence of certain factors on cognition. Analysis of this research provided insight into the mechanisms relevant to better understand and improve threat detection skills in operational settings. The primary research areas that offer potential sources of influence on threat detection capability included: attention and memory, attention and vision, change detection, decision-making, imagination and mental practice, skill acquisition, and military performance.

Based on the review, research involving the cognitive and perceptual processes of threat detection and threat detection performance (from novice to expert) was identified. For development of visual threat detection, those processes included dynamic threat monitoring, threat prioritization, and causal reasoning. The primary characteristics of threat detection involve searching the environment to identify dangerous or threatening objects and/or locations that can conceal threats. Research on attention and memory often focuses on recognition as a dual process in which the person remembering will use both broad familiarity and specific recollection cues to determine whether s/he recognizes a target. In this research, experts were expected to direct their attention more efficiently based on their familiarity with the situation and their access to more recollection cues. They should detect and identify threats rapidly because their experience allows for non-conscious processing of events. The cognitive processes that facilitate threat detection include attention to appropriate cues even when distractions are present or when there are multiple threat cues present that require attention.

A critical aspect of threat detection is noticing changes in the environment (Kowalski-Trakofler & Barrett, 2003; Staszewski, 1999). While this is critical, the research reviewed demonstrates that change detection is sometimes difficult to carry out and that human observers must direct attention to the appropriate locations in order to detect change. However, especially in the OE, seemingly insignificant changes can indicate that threat is likely. Experts are typically better at noticing changes because they tend to focus their attention on areas where threats are most likely to exist (Ericsson & Charness, 1994). Experts are predicted to be better at detecting small changes because they have witnessed such changes, experienced the threats associated with them, and understand how best to process those visual cues.

The decision-making research reviewed was concentrated on decision biases. Biases and expectations can have a direct impact across many situations that require the detection of a threat. Novice Soldiers with little to no deployment experience may miss relevant cues and focus on irrelevant cues. For instance, ignoring information that contradicts earlier judgments is a common bias. Novices enter situations with inclinations based on the procedural knowledge learned in training without having experienced the novel and unexpected events common in the real world. Experts often have biases and expectations based on their previous experiences. However, their experience handling situations that violate their expectations allows them to

⁴For the complete review, refer to Zimmerman, Mueller, and Grover (2009).

incorporate new or changing information into their current assessments of situations and re-adjust their conclusions accordingly (Kahneman & Klein, 2009).

Research on the use of visualization and mental practice to enhance performance indicates that this type of learning is effective, but only when the learner has some experience with the task or material. Cooper, Tindall-Ford, Chandler, and Sweller (2001) focused on learning by imagining and found that only students with existing schemas benefited from imagining. Similarly, reviews by Ginns (2002; 2005), indicated that prior knowledge influences the effectiveness of mental practice and visualization. Students with little prior knowledge did not benefit from these cognitive rehearsal methods while students with prior knowledge could draw on that knowledge to engage in productive visualization and mental practice. Those findings suggest a benefit in taking a tiered approach to learning threat detection. Students with little experience should study domain-relevant examples and answer practice questions in order to extend their experience base (Ginns, 2005). As students gain experience and develop schemas and mental models of events, they should further enhance their skills through cognitive rehearsal (mental practice, visualization, imagining); being able to envision the OE is most likely to benefit experienced Soldiers, but is also a good habit/skill for novices to learn.

Much research focuses on the cognitive processes required to operate in military domains. Proficient threat detection performance has been shown to be heavily influenced by both change detection and vigilance. Research comparing Soldiers of different experience levels indicates that experienced Soldiers are sensitive to subtle changes in their environments (Murphy, 2010). Signs of expertise include making global appraisals across situations and more objectively seeking information to support those appraisals, while trying to shape events in their favor (Ericsson & Charness, 1994). Research on training methods shows that game-based training enhances skills such as directing attention (Singer, Kring, & Hamilton, 2006), discrimination accuracy (Jerome, 2006), handling divided attention and improving peripheral attention (Helmuth, 2002), and altering the range of visual skills (Green & Bavelier, 2003). These findings indicate that experience influences the cognitive processes associated with effective threat detection.

Decision Models

One objective of this research was to identify the cognitive mechanisms of threat detection in order to create an expert model of threat detection. Two existing models of decision-making were used as a foundation to create the model of threat detection. One model is the OODA loop (Figure 1). The acronym OODA stands for observe, orient, decide, and act (Boyd, 1987). United States Air Force (USAF) Col John Boyd developed the OODA loop to define the nature of combat in terms of time, with both sides cycling through the OODA loop continuously and in order to disrupt the other side's cycle. His contention was that all engagements were a competition for time. The OODA loop describes the essence of combat and is present in any human conflict (Coram, 2004).

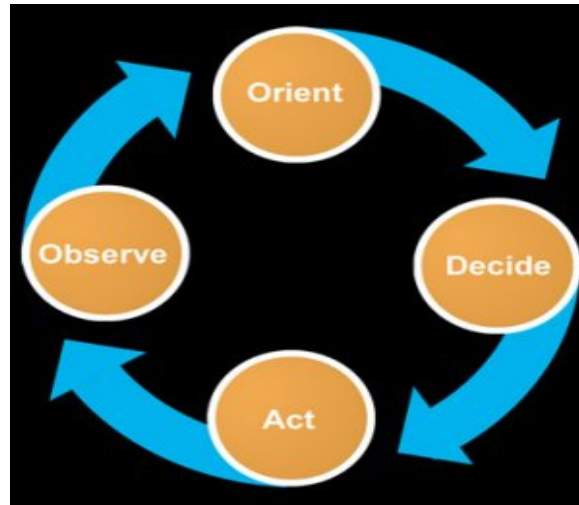


Figure 1. The OODA Loop (retrieved from <http://www.analects-ink.com/mission/OODA.htm>, March, 2010).

The first step in the decision process is to *observe* the situation, which includes receiving and assimilating information about the environment. For instance, in threat detection situations, Soldiers gather information about the people around them, the terrain, buildings and roads, and potential sources of threat. They collect enough information to interpret the situation and become oriented. If a Soldier is stuck in observation mode, no orientation takes place and s/he cannot determine what, if any, threat exists. In the *orientation* phase, decision makers construct a story about the situation based on their observations along with their previous knowledge and experiences and make assumptions about the current state of the environment. Once decision makers attain a useful understanding of the situation, they can move on to the decision phase. If they are unable to orient, or make sense of the situation, they remain “disoriented,” thus no decision is reached and they are unable to take action. In the *decision* phase, decision makers select a course of action based on their current understanding of the situation. Once the decision maker decides which action to take, they *act*. This action influences the environment, which requires decision makers to observe the situation and the cycle begins again. During this decision cycle, it is possible to skip the decision phase and go straight from orienting to action. This occurs when decision makers recognize the situation and instantly know what action to take, rather than making an effortful choice between multiple action choices.

This recognition match between the situation and action is represented in a second model and also informs the threat detection model presented in this report. The Recognition-Primed Decision (RPD) model illustrates these recognition-based decisions along with decisions that require decision makers to focus on assessing the situation (observe) or choosing a course of action (decide; Figure 2). Findings from the naturalistic decision-making literature indicate that domain-experts in time-pressured, high stakes situations tend to make decisions non-consciously, without considering all possible options. Decision makers quickly evaluate one option and imagine implementing it. If they foresee problems, they modify their plan and then implement the course of action that will suffice to avert the crisis (Salas & Klein, 2001). The decision makers in these studies generally focus on assessing the situation instead of comparing possible choice options. They tend to use mental simulations and build stories to evaluate the potential

success of their chosen action (Flin, 1996). The RPD model describes this decision process by distinguishing three levels of processing (Klein, 1998; Klein, Calderwood, & Clinton-Cirocco, 1986).

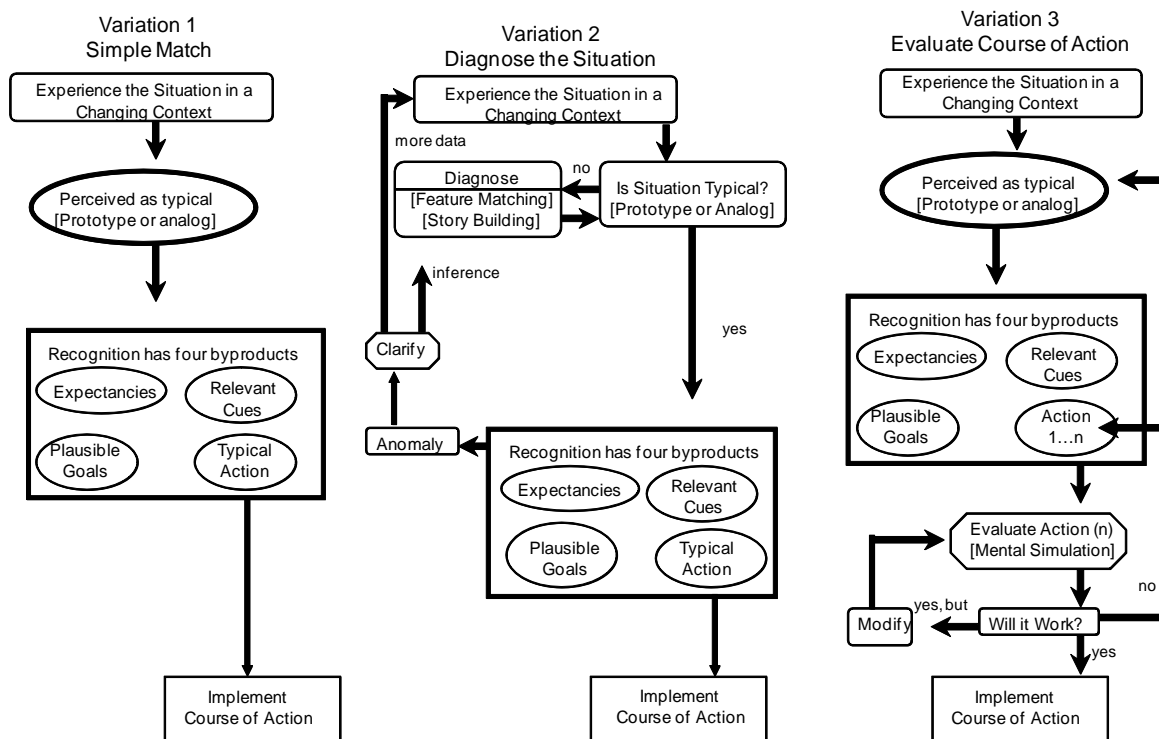


Figure 2. Three Levels of Processing in the Recognition-Primed Decision Model.

Level 1 of the RPD model represents the decision process when individuals make a simple match between the situation and the action choice. The decision maker recognizes the situation as prototypical and implements a representative action. Embedded in this assessment is the decision maker's recognition of important and usual cues, which generate expectancies about what should happen next. Based on these expectancies, plausible goals for the current situation and the typical course of action are consciously available. Level 2 represents decision-making when the situation is not so easily recognized or matched to internal representations. If the situation is unfamiliar or ambiguous, decision makers cannot rely on recognition; instead, they must assess and comprehend the novel aspects of the situation (Phillips, Klein & Sieck, 2004). This level of the RPD model focuses on situation assessment. In this case, the decision maker uses feature matching and story building to evaluate the best fitting interpretation of the situation. Level 3 diagrams the processes engaged in by decision makers who are able to assess the situation but the best course of action is not immediately clear. Therefore they must further evaluate their action choice. When individuals make action choices, they mentally simulate the possible results of implementing an action. By envisioning what may happen, decision makers predict the course of events, identify potential problems, and create alternative action plans.

In threat detection, if a Soldier identifies an obvious threat and thus realizes an obvious course of action, this represents Level 1 of the RPD model. However, when a Soldier observes

indirect evidence of a threat, it may be necessary to gather additional information to understand the situation (Level 2) or engage in further reasoning to determine the appropriate course of action (Level 3).

Expert Mental Model Development

The Threat Detection Loop

The review of the literature and the models led to the development of a qualitative model that illustrates how expertise in threat detection may emerge. This model is referred to as the *threat detection loop* (Figure 3). This model was based on theoretic models of perceptual decision-making (e.g., Mueller & Weidemann, 2008; Mueller, 2009) and traditional notions of vigilance and detection loops in applied human performance literature (i.e., Boyd's OODA loop, 1987). The intent of this model is not to supplant similar models, but rather to highlight the particular functions germane to threat detection in the OE. However, just as the OODA loop describes a continuous monitoring task, the threat detection loop describes a cyclic set of processes that capture the primary activities involved in threat detection. This model supports the hypothesis, as experience increases, observers will improve their ability to perform the skills required to detect threats effectively. The threat detection loop is a model of cognitive and perceptual processing which assists in classifying and understanding those skills of visual threat detection.

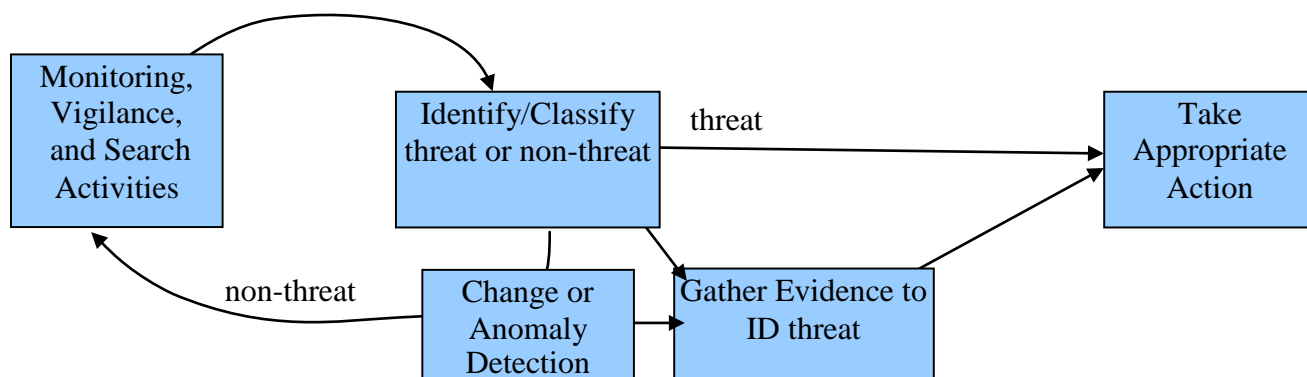


Figure 3. Diagram of the Threat Detection Loop.

One difference between this model and classic information-theoretic stage models is that there is often no clear initiation of 'input' or 'perception.' In laboratory studies, experimental trials have a clear start and a well-defined onset of stimuli. In naturalistic settings, an operator in a threatening environment may need to maintain constant vigilance, thus there is no clear start and threats may not present themselves in a well-defined manner. Representing the strategies involved in allocating attentional resources and monitoring the environment as a continual process reveals the important psychological processes involved in threat detection. Thus, the left side of the threat detection loop depicts the monitoring mode engaged in by observers as they maintain vigilance and situation awareness about a (possibly dynamic) environment.

Threat detection is characterized by three activity loops. The initial loop involves the basic monitoring and search activities required to maintain vigilance and situational awareness of the environment when no overt threats are present; it is represented by the box labeled, “Monitoring, Vigilance, and Search Activities” in Figure 3. For example, a driver may constantly survey the road ahead, the road behind, and the sides of the road to identify potentially dangerous situations, or a radar operator may monitor one or more screens for changes. Several types of events can occur to move the observer out of this inner monitoring loop. External information may emerge because of this monitoring, or in spite of it, that requires an observer to make a decision or take an action. The event may be an overtly threatening situation, such as clearly identifiable threats (the observer sees disturbed earth or a wired container), or configurations in the environment that tend to produce or disguise potentially threatening situations (roadside rubble that could indicate an attack). The information may provide evidence of a threat that is more indirect, such as an observed change from previous situations, or an anomaly (constituting a change from typicality, even if previous situations were not observed). Any of these situations may cause the observer to abort the activities constituting monitoring and engage in decision-making and/or action. However, this model does not suppose that anomaly or change detection is a necessary precursor to threat identification. Immediate events may emerge that are obvious threats or require no previous knowledge of a particular area, indicating that no change detection preceded the threat identification stage.

As suggested by the RPD model, if observers identify an obvious threat then an obvious course of action may be available (Klein, 1997). However, when one observes indirect evidence of a threat, it may be necessary to gather additional information or engage in further reasoning to determine the appropriate course of action. This is especially true for indirect signals of threat, such as changes in the environment. Observers may notice a change (perhaps a main roadway is blocked), but not know how to proceed until more information or reasoning occurs. In these situations, further reflection may either qualify the threat as real, or determine it is not an actual threat to the mission or safety. Observers may identify potential threats as non-threatening, in which case they may return to the typical monitoring processes. Qualified threats may require explicit action to intervene, but the appropriate action may require monitoring the target along with the rest of the environment. Therefore, an appropriate action may be to return to monitoring the environment, but with special attention to some perceived threat in the environment.

Observers can exit the monitoring mode in several ways to engage in other types of decisions and actions. The characteristic common to these exit conditions is that they change activity from constant monitoring for unknown threats to deliberate consideration of a particular (potential) threat. External cues or prompts may orient the observer to a particular threat. This might include communications from teammates (a driver may tell a gunner to look at specific pile of rubble), technology (a warning signal may alert a Soldier to the presence of radio frequencies associated with a remote detonation device), or an explicit threat such as an explosion may orient a Soldier to an attack location. These external cues are anomalous to the signals an observer is currently monitoring, and should have sufficient ability to capture attention.

Internal cues to exit the monitoring mode may include:

- non-conscious recognition of an overt threat (seeing a potential IED on the side of the road),
- identifying threatening situations where one might expect explicit threats to arise (upturned dirt in the road),
- detecting changes from previous observations of a situation (a normally busy market now empty), and
- detecting anomalous or atypical situations (group of people on the street in the middle of the night).

The first case is a classic example of recognition-primed decision-making (Klein, 1997). Specific objects or situations activate memory traces that allow a relatively unambiguous determination of threat. The other three conditions are more uncertain and may require more conscious and focused reasoning and information search to resolve. For example, a large class of terrain features can signal potential threats such as debris on the side of the road, chokepoints along routes, and dangerous blind alleys. Ambiguous situations that offer no explicit evidence of a threat require observers to decide whether to take action or to simply monitor and continue. When observers detect changes, they must engage in similar reasoning and decision-making activities. Changes relative to previous observations (or because of new intelligence) provide indicators of potentially threatening situations. Observers must determine whether to take action based on those changes by gathering more information and/or by reassessing the situation.

The threat detection loop provides a framework in which the primary components of visual threat detection are embedded. Initial processing of potential visual threat cues requires engagement of dynamic threat monitoring or sustaining a search in a visual environment consisting of several competing cues and distracters. This process is directly linked with classifying threats and change/anomaly detection in the threat detection loop. At this level threat prioritization occurs and threats are registered as high or low priorities; high priority threats would receive more visual attention and the observer may attempt to gather more evidence to determine if the classification is accurate. Both of these processes provide input for developing the causal inference for determining why cues might be present as is relevant to threat.

Phase I: Background Investigations

The purpose of Phase I was to acquire an initial understanding of the threat detection activities in the OE. The goals were to understand the threat detection process, including the types of threats encountered, the common cues that indicate a threat, the processes used to detect threats, and how experience enhances threat detection abilities. To do this, interviews were conducted and questionnaire responses collected from Soldiers in Phase 1a and observations of police officers on patrol were conducted in Phase 1b.

Method

Phase 1a: Preliminary data collection.

Two data collection sessions took place, each session lasting two days. For both Phase I data collections, the rank demographics are provided under the *Participants* sections and Soldiers were grouped into combat arms and combat service and service support in the *Results and Discussion* sections in order to aid discussion. Categorizing Soldiers by military occupational specialty (MOS) into combat arms and combat service/ service support was a natural and practical dichotomy for data analysis.⁵ Though not always the case, combat arms Soldiers, which include infantry and combat engineers, typically carry out missions that commonly require them to detect threats visually. This does not dismiss the fact that any Soldier may be required to rely on the skills of visual threat detection, given the situation.

Participants.

Session 1: Twenty-two U.S. Army Soldiers took part in interviews, in groups of 2-3 Soldiers; 15 were officers (1LT to MAJ) and seven were non-commissioned officers (NCO). All Soldiers were male. The mean age of the officers was 27 (range 23-34) and the mean time in service was 55 months (range 14-120). The mean age of the NCOs was 30 (range 27-37) and the mean time in service was 104 months (range 44-156). All Soldiers had deployed at least once. The threat questionnaire was not yet developed and, thus, not completed by this group.

Session 2: Twenty-one officers (all Captains) and 13 enlisted Soldiers (9 NCOs) completed questionnaires. Two officers completed only the demographic information without completing the remainder of the questionnaire and they were eliminated from the questionnaire data analysis, resulting in a total of 19 officers. All Soldiers were male. The mean age of the officers was 30.5 (range 26-41) and the mean time in service was 107 months (range 42-216). The mean age of the enlisted Soldiers was 28 (range 22-42) and the mean time in service was 91 months (range 18-156). Among these officers and enlisted Soldiers, there was a similar number of combat arms Soldiers ($n = 14$) and combat support/service support ($n = 17$). All Soldiers had deployed at least once.

Materials.

Demographic questionnaire. Soldiers in both session 1 and 2 completed the same demographic questionnaire (Appendix B). This questionnaire contained background questions, such as time in service, current rank, age, and previous deployments.

Threat questionnaire. Only Soldiers in session 2 completed a questionnaire about threat detection and threat indicators (Appendix C). The questionnaire contained three question

⁵ FM 3-0, *Operations*, (February, 2008) re-organizes the three major branches of combat arms, combat support, and combat service support into the eight elements of combat power which include the six warfighting functions: movement and maneuver, intelligence, fires, sustainment, command and control, and protection. The dichotomy of combat arms vs. combat service and service support is used in the present document because it provided the clearest distinction between Soldiers most likely to rely on and carry out visual threat detection vs. those least likely to do so.

categories and Soldiers answered by providing ratings on 5-point Likert-type scales. Soldiers rated their concern about various threats such as dangerous persons, IEDs, and vehicular threats and they rated how difficult it is to detect those threats. Finally, they rated how difficult it is to detect indicators of threats such as non-verbal behavior, roadside anomalies, and vehicle behavior.

Interview protocol. In session 1 and for the enlisted Soldiers in session 2, interviewers used a set of questions to conduct semi-structured interviews (Appendix D). The questions pertained to threats in the OE, threat detection technology, and threat detection training. Interviewers encouraged Soldiers to elaborate on their answers by discussing personal experiences.

Short-answer protocol. In session 2, the officers provided hand-written responses to a similar set of interview questions. They responded to the questions individually but in a group setting rather than one-on-one with an interviewer (Appendix E).

Procedure.

Session 1: Soldiers completed the demographic questions and then responded to the interview questions. Each session took approximately 1½ to 2 hours to complete. Soldiers answered questions about any training they had received prior to and during deployment that related to threat detection. They recounted incidents that involved the detection of threats and/or lack of detection and discussed the outcomes of these incidents.

Session 2: Soldiers completed the demographic and threat questionnaires and then responded to the interview questions. The officers completed the materials as one group. The enlisted Soldiers completed the questionnaires and interviews in groups of 2-4 Soldiers. Each session, whether completed by officers collectively or by enlisted Soldiers in small groups took approximately 1½ to 2 hours to complete.

Analysis.⁶

For the questionnaire responses, means and standard deviations were calculated for each rating scale and t-tests were used to compare combat arms Soldiers to combat support and service support Soldiers. To code the interview data, we listened to interview recordings and classified relevant interview data into pre-determined categories, such as types of threats, threat cues, and strategies for threat detection, threat detection tasks, skills, challenges, and solutions. Interviews were also reviewed to identify relevant operational experience and training involving threat detection prior to deployment.

⁶ For the Phase I (1a) and Phase II data collections: Prior to making comparisons using responses from the threat questionnaire, data were checked for normality and homogeneity of variance. All assumptions of normality and homogeneity of variance were met, unless indicated otherwise. Given that multiple comparisons were made using the same data set and due to a small sample size, a conservative approach was taken to data analysis. Attempts were made to control for Type II errors by adjusting experimentwise alpha levels using a Bonferroni correction; the new alpha level was found by dividing the original *p*-value (.05), by the number of comparisons made. A new *p*-value was calculated for each of the three major questionnaire categories (Concern, General Detection Difficulty, and Specific Indicator Detection Difficulty, with new *p*-values of .01, .01, and .006 respectively). Results that were originally significant, but not after the correction, are still reported but with the non-significance indicator, *ns*.

Phase 1a: Results and discussion.

Threat questionnaire. Ratings made by combat arms Soldiers were compared to ratings made by combat service and service support Soldiers. T-tests revealed statistically significant differences in perceptions of threat concern and specific indicator detection difficulty. In the first section of the questionnaire, Soldiers responded to the following question, “When trying to detect threat in current operational environments, how concerned are you about each threat listed?” There was a statistically significant difference between the ratings of combat arms and combat service/support in their concern for roadside IEDs. Levene’s test for homogeneity of variance was significant for that comparison, $F(1, 29) = 7.63, p < .05$, thus a t-test not assuming equal variance was used, $t(24.98) = 2.76, p = .01, r^7 = .46$. After the correction, there was not a difference between groups in their concern ratings for Vehicle Threats (Vehicle-borne Improvised Explosive Devices (VBIED), vehicle intrusions into secure locations), $t(29) = 2.00, p = .05, ns, r = .35$. Though not all comparisons were significant, combat arms Soldiers indicated higher concern ratings for the items above and for the item involving concern for dangerous persons.

Next, Soldiers rated how difficult it is to detect each of the threats within various categories by responding to the instruction to, “Rate how difficult it is to detect each of these threats.” There were no statistically significant differences between groups, but combat arms Soldiers tended to indicate higher ratings of detection difficulty on the same categories as they did for concern.

Finally, Soldiers rated how difficult it is to detect specific indicators of these threats. After the correction, there was not a difference between groups in their rating of difficulty for detecting Non-verbal Behavior (behaviors, movements, facial expressions) $t(27) = 2.58, p = .02, ns, r = .44$ and Vehicle Behavior (weighted down trunk, erratic driving) $t(28) = 2.13, p = .04, ns, r = .37$. Though not statistically significant, on all eight items measuring specific indicator detection difficulty, combat arms Soldiers indicated higher detection difficulty ratings.

Soldiers also provided comments about which threats are most difficult to detect. Their qualitative responses reflected their questionnaire responses such that dangerous persons, roadside anomalies (IED), and vehicular threats were identified as the most difficult to detect. They explained that dangerous persons are difficult to detect because they blend in with the local population, and unless they are directly engaging U.S. forces or are actively engaged in enemy activity, such as emplacing an IED, they can often go unnoticed. Combat arms Soldiers tended to focus their comments on IEDs, including VBIEDs and Person-borne Improvised Explosive Devices (PBIED), stating that these are difficult to distinguish from non-threatening items that are normally present, such as trash, pedestrians, and vehicles. They also discussed the difficulty they have in keeping ahead of the enemy’s changing TTPs, which makes it easier for the enemy to hide IEDs and exceptionally difficult to detect them. These comments reflect the experience of combat arms Soldiers. In all sections of the questionnaire, combat arms Soldiers indicated higher ratings for concern, general detection difficulty, and specific indicator detection difficulty.

⁷ In these analyses, r is a measure of effect size and can be calculated by taking the square root of the squared t-value divided by the squared t-value + the degrees of freedom. In this case, $r = \sqrt{(2.76)^2 / ((2.76)^2 + 24.98)} = .46$.

Since they, typically, have more experience detecting threats, they likely possess a better understanding of the complexity involved in filtering relevant from irrelevant information while constrained by the noise and uncertainty of the operational environment. Table 1 shows the highest mean ratings by group in each questionnaire section, which demonstrates the concern and detection difficulty for various threat types. This table illustrates a common theme around threat types including roadside IEDs, dangerous persons and vehicle behavior, regardless of classification as combat arms or combat service/service support.

Interviews. Interviews were coded according to the pre-determined categories used in the analysis of data collected in Phase II. Officers provided hand written responses to short-answer questions (Appendix E). These responses were also classified into the pre-determined categories used in Phase II. There were no systematic differences between the interview responses collected in Phase I and II. Thus, the responses from the interviews were combined into a larger data set and those results are reported under the *Phase II: Results and Discussion: Interviews* section.

Phase 1b: Expertise capture from analogous domain – Baltimore, MD police department.⁸

In addition to the academic and military literature and results from initial research, it was also informative to look at threat detection in analogous domains. Many of the operations Soldiers engage in are similar to the duties performed by police officers in domestic law enforcement. Police who patrol rural and urban U.S. streets must scan for and detect threats every day in order to deter crime, catch criminals, and protect both the community and themselves. While patrol type activities in urban environments are relatively new to Soldiers in today's OE, police officers have been attempting to detect threats on U.S. streets since formalized policing began in the U.S. in the mid-1800's (Cole & Smith, 2008).

Most police officers start their careers similar to modern Soldiers. They learn to use weapons, engage in tactical conflict, and employ proper rules of engagement (ROE) and standard operating procedures (SOP). Their first task as new officers is to patrol the streets, where they learn to differentiate threats from non-threats and how to determine the best course of action in a variety of situations. Similar to Soldiers, they must search for and monitor potential threats, distinguish between enemy and friendly civilians, manage their attention through long (10 hour) shifts, detect changes in their environments, and reason about the source and potential implications of possible threats. Both Soldiers and police officers receive some training in how to scan their environments and how to distinguish a threat from a non-threat; however, police officers do not receive training specifically aimed at threat detection. Instead, they learn from experience. Police officers typically have opportunity on a daily basis to discriminate between threats and non-threats and evaluate the likelihood and severity of threats as they decide where to expend their energies to keep their respective cities safe. This experience may provide Soldiers with insight into effective threat detection during patrol tasks.

⁸ The ARI Contracting Officer Representative (COR) obtained prior authorization for one of the contract team member's to participate in the ride-alongs.

Table 1.

Highest Mean Ratings per Threat Questionnaire Category by Groups in Phase I

Threat Detection Category	Combat Element	Items with highest mean rating	<i>M</i>	<i>SD</i>
*Threat Concern	Combat Arms	Roadside IEDs	4.64	.63
	Combat Arms	Vehicle threats (VBIEDs, vehicle intrusions into secure locations)	4.29	.83
	Combat Service/Service Support	Roadside IEDs	3.71	1.07
	Combat Service/Service Support	Vehicle threats (VBIEDs, vehicle intrusions into secure locations)	3.65	.93
**General Detection Difficulty	Combat Arms	Dangerous or malicious persons (PBIEDs or distributors of other weapons, intel gatherers)	4.07	.62
	Combat Arms	Vehicle threats (VBIEDs, vehicle intrusions into secure locations)	3.93	.92
	Combat Service/Service Support	Vehicle threats (VBIEDs, vehicle intrusions into secure locations)	3.69	.70
	Combat Service/Service Support	Roadside IEDs	3.63	.89
**Specific Indicator Detection Difficulty	Combat Arms	Vehicle Behavior (weighted down trunk, erratic driving) that indicates smuggling (weapons, persons)	3.71	1.07
	Combat Arms	Roadside anomalies (upturned dirt, packages, out-of-place vegetation) that indicate enemy presence (attack or surveillance)	3.43	.85
	Combat Service/Service Support	Items in buildings (explosive materials, Intel) that indicate terrorist activity	3.00	1.04
	Combat Service/Service Support	Roadside anomalies (upturned dirt, packages, out-of-place vegetation) that indicate roadside explosives	2.88	1.09

Combat Arms $n = 14$, Combat Service/Service Support $n = 17$.

*For the items involving Threat Concern, the response scale ranged from, 1 = Not at all concerned to 5 = Extremely concerned.

**For the items involving General Detection Difficulty and Specific Indicator Detection Difficulty, the response scales ranged from 1 = Not at all difficult to 5 = Extremely difficult.

Participants. Three patrol officers from the Baltimore, MD, Police Department participated by allowing one researcher (Zimmerman) to ride with them during half of their normal patrol shifts (10 hours). Ride-alongs were conducted on three separate days as shown in Table 2:

Table 2.

“Ride-along” Schedule

Ride-along Time	Participant #	Yrs Experience	Rank
1500-2000	Officer 1	2	Patrol Officer
1800-2300	Officer 2	9	Acting Sgt
0700-1200	Officer 3	10	Patrol Officer

Procedure. Officers volunteered to host a ride-along at the request of their supervisor. The researcher arrived at the appointed time, was issued a bulletproof vest, and signed a liability waiver. Each officer signed an informed consent form. The researcher explained the purpose of the ride-along was to understand threat detection in high-threat patrol situations so officer experience and knowledge could support better understanding and development of a training exemplar for Soldiers in operational settings. Activities during the ride-along included going to calls-for-service, patrolling streets, meeting with other officers, and discussing threat detection while on patrol. The researcher took notes and asked questions about threat detection in police activities observed during the ride-along, in previous experiences, and in general. At the end of each ride-along, the officer took the researcher back to the police station and the officer was allowed to ask any remaining questions about the project.

Phase 1b: Results and discussion.

Patrol environment. All notes taken during the ride-alongs were typed up and the observations and activities are reported in Appendix F. The ride-alongs took place in the Northwestern district of Baltimore, MD. This is a high-drug, high-crime, low-income section of Baltimore, MD. It is one of the largest districts in Baltimore with a diverse population and a high police presence. Officers indicated that it is the second most dangerous district in Baltimore. The predominant threat to officers is people armed with guns, which is a particular concern in this area due to high drug and gang activity.

Relevance to military patrol activities.

Many similarities exist between police and military patrol environments. Key tasks for Soldiers in the OE are to build relationships in the community, befriend the children, elicit information from sources and community members, and demonstrate a “presence” to lower criminal activity. The officers in this research also engaged in these activities. They discussed threat indicators similar to those provided by Soldiers, such as people leaving the area when police are around, non-verbal signs of nervousness or uneasiness, activities that are out of place, and items in the street that are meant to detour police.

As shown in Appendix F, the difference in experience between Officer 1 compared to Officers 2 and 3 provides evidence for understanding experience-related differences in threat detection. Officer 1 showed less discrimination between threats and a lower criterion for responding to threats. Officer 2 and Officer 3 discriminated between threats and had a much higher threshold when choosing which threats were worth a response. Officer 3 demonstrated high skill in visual search and attention, anomaly detection, and the use of mental models and experience. He “went with his gut” to respond to subtle cues and then would seek out information to confirm or disconfirm his initial reaction. These are the skills that are especially relevant to novice Soldiers conducting patrols, because they encompass the necessary skills of detecting threats in operational settings. In both visual threat detection environments, we would expect as police officers and Soldiers become more experienced their response criterion for various potential threats shifts from being simply reactive to being selective and accurate. Likewise, as the Soldier’s ability to prioritize and reason about relevant information and filter irrelevant noise becomes more efficient, the associated response becomes more precise.

Discussion: Background investigations.

The background investigations provided information about threat detection situations and activities in the OE as well as provided insight into possible differences in threat detection performance based on experience. An account of patrol activities of police officers also provided insight into situations with high threat likelihood. The results from this research, especially Soldier comments, support the conclusions made in the literature review about the importance of threat search, change detection, and attention management when trying to detect threats. For instance, Soldiers emphasized the complexity of threat environments, stating that it is difficult to see everything and that the enemy continually changes TTPs. Self-reports show that Soldiers have greater concern for the threats that are most relevant based on their experience, and that they are more likely to detect, such as dangerous persons, roadside IEDs, and vehicle threats. Responses revealed a trend such that combat arms Soldiers collectively provided higher ratings for concern, general detection difficulty, and specific indicator detection difficulty. Though only self-report measures, they revealed differences in experience via trends of more and less combat experienced Soldiers. Therefore, the research was focused on understanding the detection of the more common threats and identifying how to improve the skills necessary for detection of those prominent threats.

Observations of police officers provided examples of threat detection as it occurred in their patrol environments. Those environments required constant vigilance to detect, assess,

filter, and react to potential threats. The findings demonstrate the possible differences in threat detection processes of less and more experienced officers. The less experienced officer responded readily to many potential threats without much differentiation based on threat severity. The more experienced officers evaluated possible threats with little deliberation and judged threat severity and probability of effective outcomes based on their existing knowledge and experience.

These findings are similar to those found in the expertise literature, which indicates that expert decision makers quickly form mental representations of the problem, allowing them to make quick and accurate decisions. Studies show that, compared to their novice counterparts, domain experts are better able to perceive and process information, recognize pertinent cues, and match those cues to previous experiences in a manner that facilitates successful action (Ericsson & Charness, 1994; Goodrich, Sterling, & Boer, 2000). Dreyfus and Dreyfus (1986) contend that as expertise develops, decision makers begin to perceive situations as a whole, rules become less important, and decision makers become more flexible and react faster to incoming information. Observations indicated that these findings may apply to threat detection experience and this provided evidence for refining experimental materials and for further developing the threat detection loop in Phase II.

Phase II: Pilot Test

The purpose of Phase II was to gather further information about threat detection skills to develop experimental materials and methods, develop an expert mental model of threat detection, and test a preliminary version of the computer-controlled exercise. In this research, we gathered more information about potential threats by having Soldiers identify threat locations in several photos and topographical maps, rate likelihood and severity of these threats, and provide their reasoning about each location they chose. They also responded to questionnaires and participated in interviews.

Method

Data collection.

Participants.

Twenty-five Soldiers, 10 officers (2LT to CPT) and 15 enlisted Soldiers (10 NCOs) took part in this data collection. All Soldiers were male. The mean age of the Soldiers was 30 (range 21-48) and the mean time in service was 96 months (range 24-252 months). Three of the Soldiers had not deployed, but all other Soldiers had deployed at least once.

To match analysis in Phase 1a, Soldiers were grouped into either combat arms ($n = 12$) or combat service and service support ($n = 13$). The data were analyzed separately and then combined with data from Phase 1a for an overall analysis of questionnaire responses.

Materials.

Demographic and threat questionnaires. The demographic questions and the threat questionnaire were the same as those presented to Soldiers who participated in Phase I (see Appendices B and C).

Imagery analysis. The purpose of this exercise was to gather general assessments of threat in different situations. Special-purpose software using the Psychology Experiment Building Language (PEBL) 0.09 computer experimentation system controlled the computer exercises (Mueller, 2009). Ten images were selected to cover a range of potential threat situations, such as topographical maps, aerial imagery, and ground-based photos (Appendix G). These images came from U.S. Topographic maps, freely available pictures published by U.S. Department of Defense (DoD) contractors on their web sites (e.g., <http://uspi.us/Photos>), and screen captures from U.S. DoD video sources.

Interview protocol. Interviews were conducted to gather information about threat detection processes and the skills developed through training and experiences within the OE. Questions focused on recent threat detection experiences during mounted and dismounted urban patrols in Operation Enduring Freedom (OEF) or Operation Iraqi Freedom (OIF). Soldiers also identified the critical components of threat detection and the threat detection skills that develop with experience (Appendix H).

Procedure.

The pilot test involved two main parts: a computer-controlled exercise sequence and a semi-structured interview. The computerized exercises took place first and lasted between 30 and 45 minutes. The interviews lasted approximately one hour.

At the start of each session, Soldiers received a description of the exercises and an explanation that the purpose of the project was to capture their threat detection experiences and identify common threat detection situations, indicators, and challenges in the OE. Soldiers then completed the computer exercises at their own pace. They could ask clarification questions during any part of the session.

During the imagery analysis exercise, Soldiers viewed 10 images (one at a time) and annotated the (potential) threats they perceived in each image. A brief background story for each image was provided. The Soldiers proceeded through the exercise by viewing each image and clicking with the mouse pointer on locations they judged to be of greatest threat. After clicking on a location, Soldiers selected the likelihood of actual threat using a three-level scale (low = yellow, medium = orange, high = red) and then indicated severity of the threat in that location using the same three-level scale (low = yellow, medium = orange, high = red). Following this, they typed a short annotation describing the threat. The computer displayed a circle in the clicked-on threat locations and added the typed note in a text box on the right side of the screen (Figure 4). Soldiers could identify any number of threats and make unlimited annotations, with no upper or lower limit constraints. They provided between three to 10 points of interest per image. Each Soldier viewed the images in the same order.

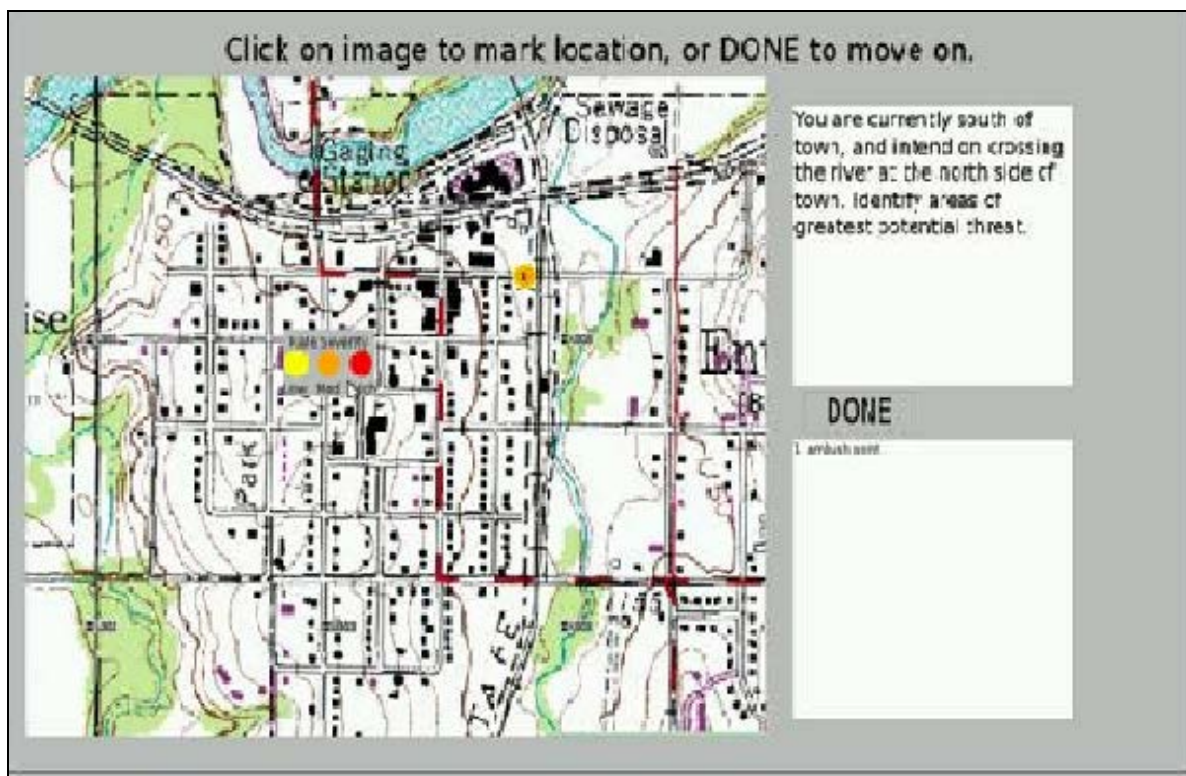


Figure 4. Imagery Analysis Exercise Screen Shot.

Following the computerized exercises, Soldiers engaged in a one-on-one interview that lasted approximately 40 to 80 minutes. At the end of the session, Soldiers could ask questions and make comments about the experiment and the project. Soldiers were debriefed and contact information for mental health assistance provided to them. They could use this contact information if discussion of their experiences brought up any negative feelings or memories.

Analysis.

Threat questionnaire. For questionnaire responses, the mean ratings and standard deviations for combat arms and combat support/service support Soldiers were computed and t-tests conducted to determine if their responses differed. These data were then combined with data from Phase 1a and analyses conducted to determine if overall differences existed (across data collections) between combat arms and combat service/service support Soldiers.

Imagery analyses. For the data from Soldiers' imagery analyses, the type and amount of targets clicked by Soldiers on each image was analyzed (Appendix I). A linguistic analysis of the text annotations was performed to identify common and recurring themes in the types of threats identified (Appendix J). The correlation between the two 3-level ratings given to the annotations (likelihood and severity) was assessed as were the annotation patterns on particular images to identify specific regions-of-interest for threatening or suspicious locations in the

current imagery set and for general themes of threatening situations that could be identified in other imagery.

Interviews. The interview recordings were reviewed and classified into pre-determined categories, including types of threats, threat cues, and strategies for threat detection, threat detection tasks, skills, challenges, and solutions. The interview data from Phase 1a were incorporated into data from Phase II.

Phase II: Results and Discussion

Threat questionnaire.

In the first section, Soldiers responded to the question, “When trying to detect threat in current operational environments, how concerned are you about each threat listed?” As with the findings in Phase I, after the correction, there was not a difference between groups on Roadside IEDs, $t(23) = 2.04$, $p = .05$, *ns*, $r = .39$ or between groups on the concern rating for Vehicle Threats (VBIEDs, vehicle intrusions into secure locations), $t(23) = 2.21$, $p = .04$, *ns*, $r = .42$. Though not statistically significant, combat arms Soldiers indicated higher concern ratings.

Soldiers also rated how difficult it is to detect each threat by responding to the instruction, “Rate how difficult it is to detect each of these threats.” There were no statistically significant differences between groups on those ratings. Finally, Soldiers rated how difficult it is to detect specific indicators of these threats. Again, there were no statistically significant differences between groups on those ratings. Combat arms Soldiers tended to indicate higher ratings of concern and indicator detection difficulty.

These results are similar to those indicated in Phase 1a questionnaire responses. For the majority of ratings involving concern, detection difficulty, and specific indicator detection difficulty, combat arms Soldiers indicated higher levels of concern and detection difficulty. Combat arms Soldiers are more likely to be in the positions (e.g., gunner position in a vehicle) that require scanning for vehicle threats in a noisy operational setting. Urban settings in particular are full of vehicles of many makes, models, and conditions all of which can serve as a primary method for executing severe attacks (VBIED). Thus, we would expect the self-reported magnitude of these threats to be higher for those Soldiers with more experience carrying out such responsibilities. Vehicles can carry large amounts of explosives, may often go undetected, and can quickly gain access to Soldier positions. Soldiers echoed this concern in the Preliminary Experiment where one of the photos selected by multiple Soldiers for further discussion was one depicting a vehicle at a checkpoint. Table 3 shows the common concern and detection difficulty ratings across groups. This global view represents a similar result as the first data collection; the commonly identified threat types included roadside IEDs, dangerous persons and vehicle behavior.

Table 3.

Highest Mean Ratings per Threat Questionnaire Category by Groups for Phase II

Threat Detection Category	Combat Element	Items with highest mean rating	<i>M</i>	<i>SD</i>
*Threat Concern	Combat Arms	Roadside IEDs	4.50	.67
	Combat Arms	Dangerous or malicious persons (PBIEDs or distributors of other weapons, intel gatherers)	4.17	1.12
	Combat Service/Service Support	Roadside IEDs	3.85	.90
	Combat Service/Service Support	Dangerous or malicious persons (PBIEDs or distributors of other weapons, intel gatherers)	3.62	.65
**General Detection Difficulty	Combat Arms	Dangerous or malicious persons (PBIEDs or distributors of other weapons, intel gatherers)	3.83	.72
	Combat Arms	Roadside IEDs	3.33	1.30
	Combat Service/Service Support	Vehicle threats (VBIEDs, vehicle intrusions into secure locations)	3.77	.93
	Combat Service/Service Support	Roadside IEDs	3.62	1.12
**Specific Indicator Detection Difficulty	Combat Arms	Items in buildings (explosive materials, intel) that indicate terrorist activity	3.42	.90
	Combat Arms	Roadside anomalies (upturned dirt, packages, out-of-place vegetation) that indicate enemy presence (attack or surveillance)	3.25	.97
	Combat Service/Service Support	Vehicle Behavior (weighted down trunk, erratic driving) that indicates smuggling (weapons, persons)	3.46	.78
	Combat Service/Service Support	Roadside anomalies (upturned dirt, packages, out-of-place vegetation) that indicate roadside explosives	3.23	1.01

Combat Arms $n = 12$, Combat Service/Service Support $n = 13$.

*For the items involving Threat Concern, the response scale ranged from, 1 = Not at all concerned to 5 = Extremely concerned.

**For the items involving General Detection Difficulty and Specific Indicator Detection Difficulty, the response scales ranged from 1 = Not at all difficult to 5 = Extremely difficult.

Combined analysis: Phases I and II.

A two-way Analysis of Variance (ANOVA), using location (Phase 1a and Phase II) and combat element type (combat arms vs. combat support/service support) as between-subjects factors revealed no main effects nor significant interaction. Therefore, data from Phase I and Phase II were combined to provide an overall perspective, across data collections, between combat arms Soldiers ($n = 26$) and combat support/service support ($n = 30$).

After the Bonferroni correction (see page 12), there was not a difference between groups on ratings of concern, dangerous or malicious persons (PBIEDs or distributors of other weapons, intel gatherers) $t(54) = 2.44, p = .02, ns, r = .32$. There was a statistically significant difference between groups on the concern rating for Roadside IEDs. Levene's test for homogeneity of variance was significant for that comparison, $F(1, 54) = 6.41, p < .05$, thus a t-test not assuming equal variance was used $t(48.40) = 3.48, p = .001, r = .45$. There was also a statistically significant difference between groups on Vehicle Threats (VBIEDs, vehicle intrusions into secure locations), $t(54) = 2.95, p = .005, r = .37$. In those ratings, combat arms Soldiers indicated higher concern ratings. There was one difference between groups on the detection difficulty rating, dangerous or malicious persons (PBIEDs or distributors of other weapons, intel gatherers). Levene's test for homogeneity of variance was significant for that comparison, $F(1, 53) = 15.61, p < .05$, thus a t-test not assuming equal variance was used, after the correction, $t(45.18) = 2.06, p = .05, ns, r = .29$; again, combat arms Soldiers indicated higher ratings, though not statistically significant by the conservative standard employed in the analysis. There were no differences between groups on any of the indicator detection difficulty ratings.

Overall, combat arms Soldiers provided higher ratings for each of the threat questionnaire categories (concern, general detection difficulty, and specific indicator detection difficulty). In some of the results, Soldiers in combat support and service support did indicate ratings as high as combat arms Soldiers in each of the three categories. Upon further review, those Soldiers who were originally trained for combat support or service support roles, had actually performed combat arms activities on their most recent deployments.

In addition, interviews with Soldiers trained primarily as cooks, mechanics, and armor crewmen all revealed that they had primarily been involved in conducting dismounted patrols (or similar activities), as the mission required. Regardless of the branch classification and training qualification, Soldiers from combat arms and combat service/service support have been required to conduct missions that require a strong reliance on visual threat detection skills.

In general, both groups of Soldiers indicated moderate to high ratings of concern and detection difficulty across items. Such results demonstrate a common reflection of how challenging it is to sift through the sheer amount of information and noise in the operational environment to find threats that vary in their probability of occurrence. Table 4 provides the highest mean ratings per questionnaire section (threat concern, general detection difficulty, and specific indicator detection difficulty) by groups for the combined data set. Not surprisingly, the combined findings suggest that roadside IEDs or anomalies, dangerous persons, and vehicle threats were of most concern and most difficult to detect.

Table 4.

Highest Mean Ratings per Threat Questionnaire Category by Groups in Phases I and II

Threat Detection Category	Combat Element	Items with highest mean rating	<i>M</i>	<i>SD</i>
*Threat Concern	Combat Arms	Roadside IEDs	4.58	.64
	Combat Arms	Vehicle threats (VBIEDs, vehicle intrusions into secure locations)	4.19	.90
	Combat Service/Service Support	Roadside IEDs	3.77	1.07
	Combat Service/Service Support	Dangerous or malicious persons (PBIEDs or distributors of other weapons, intel gatherers)	3.53	.86
**General Detection Difficulty	Combat Arms	Dangerous or malicious persons (PBIEDs or distributors of other weapons, intel gatherers)	3.92	.56
	Combat Arms	Vehicle threats (VBIEDs, vehicle intrusions into secure locations)	3.88	.82
	Combat Service/Service Support	Vehicle threats (VBIEDs, vehicle intrusions into secure locations)	3.72	.80
	Combat Service/Service Support	Roadside IEDs	3.62	.98
**Specific Indicator Detection Difficulty	Combat Arms	Vehicle behavior (weighted down trunk, erratic driving) that indicate smuggling (weapons, persons)	3.46	1.10
	Combat Arms	Roadside anomalies (upturned dirt, packages, out-of-place vegetation) that indicate enemy presence (attack or surveillance)	3.35	.89
	Combat Service/Service Support	Vehicle behavior (weighted down trunk, erratic driving) that indicate smuggling (weapons, persons)	3.14	.99
	Combat Service/Service Support	Items in buildings (explosives materials, Intel) that indicate terrorist activity	3.04	1.13

Combat Arms $n = 26$, Combat Service/Service Support $n = 30$.

*For the items involving Threat Concern, the response scale ranged from, 1 = Not at all concerned to 5 = Extremely concerned.

**For the items involving General Detection Difficulty and Specific Indicator Detection Difficulty, the response scales ranged from 1 = Not at all difficult to 5 = Extremely difficult.

Imagery Analysis

Annotations.

The annotation patterns on particular images provided specific regions-of-interest for threatening or suspicious locations in the imagery set and provided general themes of threatening situations that may generalize to other imagery. The annotations assisted in the identification of high-likelihood and low-likelihood threat locations to inform later experiments.

Annotation example.

One image that Soldiers analyzed was a topographical map of a small, unidentified town (see Figure 5). Soldiers read the following lead-in:

You are currently south of town and intend on crossing the river at the north side of town. Identify areas of greatest potential threat.



Figure 5. Annotation Example.

An identifier marks each clicked-on location (e.g., #109 on the left in Figure 5). Soldiers provided an annotation for each identifier (Appendix J). The colored rings around each identifier specify the likelihood and severity ratings: 1 (least likely) = yellow, 2 = orange, or 3 (most likely) = red, with severity ratings indicated on the outer ring and likelihood ratings indicated on the inner ring. Very few annotations differed in these ratings (e.g., #18 on the middle left has an

orange inner ring and a red outer ring). Annotations concentrated on the most likely route through the village. Soldiers focused on the north end of the map where larger buildings are located next to a river crossing, which represented a chokepoint. According to the lead-in, Soldiers had to use this crossing, making the enemy more likely to use this as an ambush point; the enemy could easily cut off escape routes and inflict focused damage on coalition forces.

The two 3-level ratings (likelihood and severity) given to the annotations were highly correlated ($R = .71$, $t(707) = 27$, $p < .01$). In 574 out of 709 cases (81%), the ratings were identical. Table 5 shows the cross-tabulated dependencies between these two measures. Such results could arise if the most common threats were actually the most dangerous. We suspect that this is not the case and the opposite may in fact be true. The least severe threats, such as intelligence gathering by the local populace, may be the most common. These results may have occurred because the task of annotating threats places a criterion on the task. Or, Soldiers may naturally evaluate threats in a utility sense by incorporating both likelihood and cost, and are unable to disentangle the two notions. This idea is supported by the fact that the likelihood ratings and the severity ratings were largest when those levels matched; following diagonally across Table 5, the largest counts occur in cells of matching levels of likelihood and severity (e.g., 85, 318, and 171, respectively). A third possibility is that the types of threats discussed are all very rare and in follow-up interviews we typically found that although such threats were always (potentially) present, attacks by enemies or from IEDs happened infrequently; for some Soldiers they occurred only a few times per tour. Because the likelihood dimension for ultra-rare events may be essentially meaningless, Soldiers may use severity as a stand-in for likelihood.

Table 5.

Cross-tabulation of Likelihood and Severity Ratings across All Images

Severity	Likelihood*		
	1	2	3
1	85	29	2
2	25	318	13
3	16	50	171

*Likelihood ranged from 1 = *least likely* to 3 = *most likely*.

Similarly, Severity ranged from 1 = *least severe* to 3 = *most severe*.

Soldiers identified between zero and 10 targets per image, with a mean of 2.95. Soldiers identified no threats only when they accidentally hit the “done” button and the computer program did not allow them return to the previous image. Those trials were excluded from any analyses. The ten images used in the exercise received between 44 and 118 annotations per image across all Soldiers.

A linguistic analysis of the text annotations was performed to help identify common and recurring themes in the types of threats identified. First, we removed function words (e.g., “and,” “the”) and word differences based on tense (“IED” and “IEDs”). We combined misspellings (“maneuver” vs. “manuever”). The total number of different words used in the annotations was 1185. This allowed for a calculation of the frequency of usage for each distinct word. The words indicated most often included those referring to common threats (“IED,” “sniper,” “enemy,” “ambush”), those making reference to abstract or specific locations, geography or architecture (“location,” “point,” “position,” “bridge,” “building”), and those reflecting the non-deterministic nature of threats (“possible,” “potential”). Given these results, the language reflects expectations about threats and their potential locations as well as the uncertainty embedded in the operational setting. See Appendix K for a complete list of words used more than twice (276 words total) sorted by number of occurrences.

Interviews.

The results of the interviews conducted at Phase 1a and Phase II provided guidance for refining the research materials. The information that Soldiers provided and the experiences they recounted lent support to the cognitive processes highlighted in the literature review as well as responses to the threat questionnaire and computer exercises. Below are some of the primary comments provided by Soldiers concerning challenges and indicators.

Comments about threat detection challenges:

- it is difficult to see everything that could be a threat,
- it is hard to stay vigilant on long operations,
- even with training and rehearsing, Soldiers can only react to threats like IEDs,
- smaller units must occupy areas larger than they can handle given their amount of resources,
- more damaging threats are concealed better, making them harder to detect,
- the enemy is constantly shifting their TTPs making it difficult to adapt,
- it is difficult to detect VBIEDs,
- it is difficult to tell definitively if persons are a threat or not, and
- no two areas of operations are the same.

Comments about detecting threat indicators:

- soldiers need to notice and understand changes in the local area and people,
- it is important to pay attention to the local population’s reaction to Coalition Forces,
- it is possible to conceal (IED) threats in almost anything: the ground, in cars, on persons, in trash, roadside rubble, newly constructed sidewalks, etc.,
- soldiers need to recognize components of IEDs, such as cell phones, timers, wire, etc.,
- if people (or children) are not around as expected, given the location and time of day, Soldiers should be vigilant,
- the enemy can reuse previous holes/craters for new IEDs, and
- citizens appearing agitated or not wanting to talk (could indicate a threat is imminent).

The interview responses were classified into the categories presented in Table 6. These results provided direction for further investigation in the pilot testing and initial experimentation. According to self-reports, all types of threats are difficult to detect, but the concern is greater for dangerous persons, roadside IEDs, and vehicle threats. Threat indicators are also difficult to detect and this helped in the determination to present a wide variety of indicators to Soldiers in the experimental phases. Presenting different indicators allowed an assessment of any differences in threat detection performance based on experience, across or between different indicators. The characteristics of operational settings and threat indicators identified by Soldiers provided guidance on the threat detection stimuli developed for the pilot test.

Table 6.

Interview Data Categories

Interview Data Classification	High-level Categories
Types of Threats	Enemy activity, enemy tactics, environmental cues, troop activity, crowd behavior
Threat Cues	Behavioral cues, environmental cues, physical cues (such as wires, garbage), patterns of cues
Strategies for Threat Detection	Tactics, information gathering, spot cues, spot trends, ask what-if questions
Threat Detection Tasks	Scan environment, question subjects, active evidence search, observe situations and environments
Threat Detection Skills	Think like the enemy, prioritize information, aggregate information, form mental picture of situation, ask what-if questions
Challenges in Detecting Threats	Noticing cues, noticing patterns, enemy TTPs, information reliability, night operations
Threat Detection Training/Preparation	Scenario-based training, train consequences, use Iraqi/Afghan role-players/environments, think like the enemy, real-world experience, what-if questions

Many Soldiers emphasized the importance of experience in detecting threats. Much of what Soldiers know about threat cues and about strategies for assessing and dealing with threats they learned while conducting missions or from other Soldiers with operational experience. This indicates that differences in performance should be expected based on the experience level of the threat detector. Soldiers emphasized the importance of training scenarios that are realistic and experiential, further highlighting the importance of experience in skill development.

Soldiers discussed threat detection activities that reflect many of the cognitive processes discussed in the literature review. For instance, Soldiers discussed the importance of gathering information and spotting relevant cues. They described threats, threat cues, important threat information, and challenges to conducting threat detection in operational environments. Examples of quotes from the interviews are included in Appendix L. With focus on dynamic threat monitoring, threat prioritization, and causal reasoning, as well as examples of relevant threats, threat cues, and challenges from the interviews were used to create experimental environments and manipulations that test for differences between novice and expert threat detectors. This knowledge allowed for the creation of contextually rich and relevant research stimuli for more valid testing of threat detection skills and cognitive processes. In addition, the information gleaned from this phase contributed to the further development of the expert mental model of threat detection.

Plan for Testing the Model of Expert Threat Detection

To prioritize and choose metrics for experimental testing, the findings from Phase I were used to guide method development in Phase II. The imagery analysis exercise allowed Soldiers to identify areas of potential threats and annotate why these areas were a concern. This analysis provided information about the regions of interest, threat cues, and explanations about the threats. From this, materials were created to measure dynamic threat monitoring, threat prioritization, and causal reasoning about threat environments.

Questionnaire ratings were similar to those provided by Soldiers in Phase 1a. Combat arms Soldiers tended to indicate higher levels of concern and difficulty across the different types of threats, with the most concern being for relevant operational threats such as IEDs and suspicious persons and vehicles. The interview data were classified into several categories and the analysis focused on the tasks and skills required to detect threats in the OE. Soldiers discussed how they gather information, spot cues and trends, scan environments, observe changes, aggregate data, and form mental pictures of situations. Based on experience, they described the types of threats and cues present in threat situations. That information was used to develop the stimuli and to inform the exercises Soldiers would complete in the future experiments.

The plan for developing and testing the model of expert threat detection was based on the hypothesized threat detection loop presented in Figure 3 (pg. 8). The goal was to develop experimental measures that would determine expert-novice differences in threat detection and identify the skills possessed by expert threat detectors. How expertise may facilitate different processes in the threat detection loop is shown in Figure 6. The results from Phases I and II supported the development of that threat detection mental model. That model illustrates the

threat detection process and current findings suggest that experience and knowledge influence and facilitate the threat detection process. The role experience plays in each of the steps in the threat detection loop was defined as were the measurable behaviors associated with each of these roles. Defining these behaviors allowed an identification and prioritization of the metrics to be measured in the experiment.

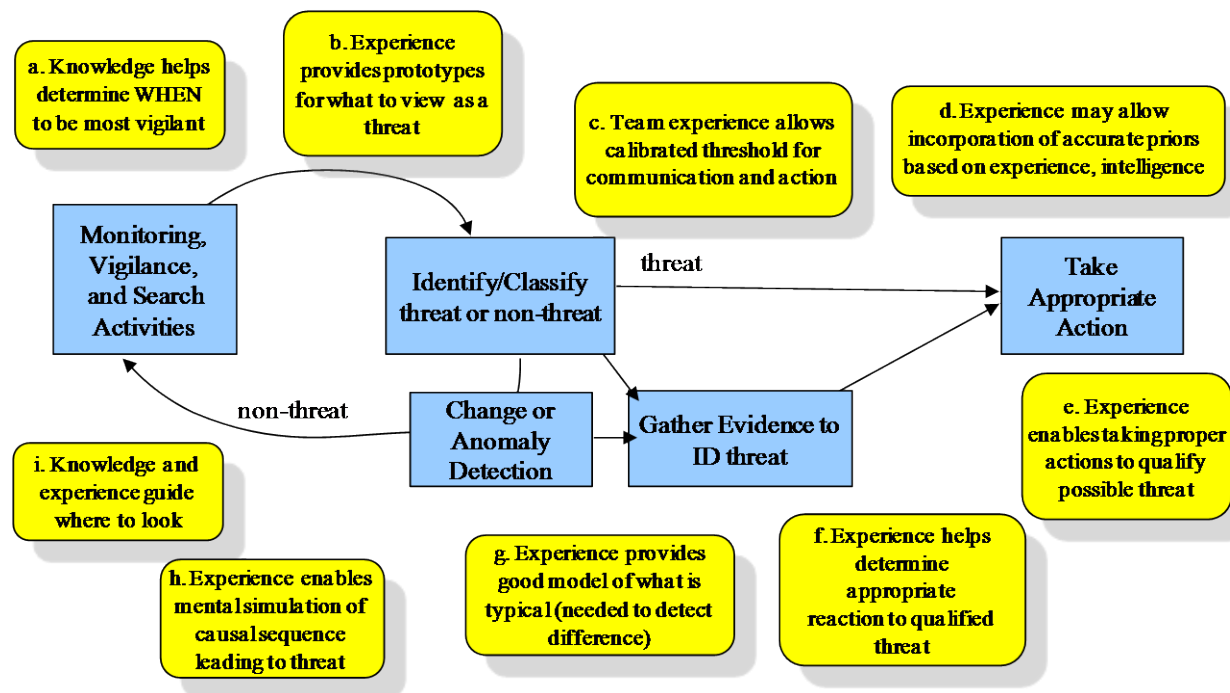


Figure 6. The Influence of Experience, Knowledge, and Expertise on Threat Detection Processes.

The outer boxes in Figure 6 demonstrate the role experience, knowledge, and expertise play in the functions of the threat loop. For example, while monitoring a situation for threat, experience and knowledge can help guide what to look for (b), when to be most vigilant (a), and where to spend the most time looking (i). Knowing how to look for threat may result from direct experience, but may also come from the current intelligence of the day. Expertise may manifest in knowing how to look, but also in how to use available knowledge to guide visual search. To illustrate this distinction, consider an explosive device hidden in a roadside curb. Experts may know from previous experience to look at curbs for signs of attack, but even if this is a new method of attack, experts may be more apt, relative to novices, to incorporate warning from an intelligence briefing about curb-based attacks into their threat detection activities.

Knowledge about what to look for carries forward in the threat detection process. Experts have existing knowledge of potential threats that facilitates non-conscious classification of information and suggests appropriate courses of action (cf., Klein, 1997). However, the interviews conducted as part of this research revealed occasions when potential threats that never materialize overshadowed overt threats. Without the ability to select the correct potential threat to act upon, inaction may paralyze a patrol. In these cases, we hypothesize that the observer makes a decision by weighing the evidence, considering background probabilities of threat (d),

and creating causal-based stories about how the threat may manifest in the observed situation (h). We hypothesize that type of decision is akin to those described in Mueller's (2009) Bayesian Recognitional Decision Model. The current model allows observers to establish a flexible decision threshold. Thresholds for action may depend on agreed upon norms of a team (c), or be based on learned tactics and judgments about the situation (f).

Finally, expert knowledge facilitates threat detection by improving change detection or anomaly detection (g). Change detection requires one to have prior experience with an environment, either first-hand or second-hand via word-of-mouth, intelligence materials, or other sources. A Soldier who notices that a usually open store has closed early may interpret this change as a potential threat. Similarly, anomaly detection is a type of change detection in which one identifies violations of expected normality, even when no exact memory of the situation exists. Experts have a richer understanding of what is typical and atypical, and are often better able to detect anomalies.

Measurable expert behaviors.

Figure 7 provides a set of potentially measureable behaviors that indicate expertise influence on threat detection; these behaviors are metrics of expertise. To determine how behaviors contribute to threat detection, the research data revealed several real-world behaviors that can be simulated in exercises or laboratory settings. The annotations in Figure 7 roughly correspond to the annotations in Figure 6. For example, knowing where and when to look in a situation (Figure 6, a) should help an expert encode details about a situation (Figure 7, a) and maintain better situation awareness. Also shown in Figure 7, experts should be able to see patterns during visual search that are consistent with deeper understanding of the situation and sensitive to priors, expectations, and causal reasoning (i). Related to this is the ability to construct causal stories about situations (h), especially related to how certain threats might materialize. An expert understanding of visual features related to threat would enable better and faster classification of these situations (b).

Because experts need to be selective about what they respond to, we hypothesize that they should be able to adapt this selectivity to the situation (c), akin to the way signal detection theory (SDT) supposes a threshold may change (See Green & Swets, 1966). Similarly, prior suspicion and causal reasoning about a threat (d) should influence decision-making. Experts should be able to determine whether evidence is strong enough to take action or if more information must be gathered (f), and identify appropriate courses of action after they decide to take action (e). Finally, experts should be better able to detect changes or anomalous events in a situation (g).

These behaviors can be measured in simulated threat situations to assess expert-novice difference in the abilities. As part of the research plan, metrics were identified that measure the behaviors represented in Table 7. These metrics were then prioritized and a set of research procedures identified to measure expert-novice differences.

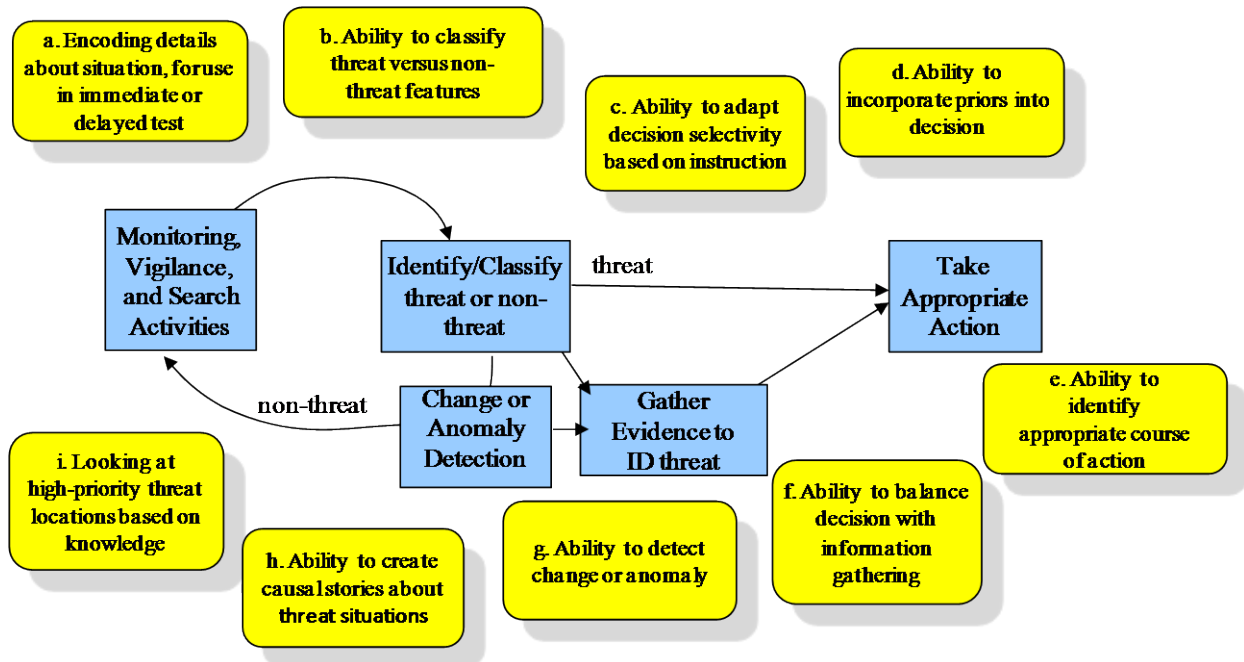


Figure 7. Measurable Behaviors of Experts in the Threat Detection Loop.

Metrics of expertise.

Table 7 presents the metrics corresponding with each measureable behavior associated with expertise in threat detection. Deciding which metrics to measure required some cost-benefit analysis and pilot testing, as determined by the research team. Costs include the number of Soldiers (expert and novice) required to find reliable differences, the effort involved in developing testing paradigms and stimuli, potential equipment needed to collect the metrics, and the extent to which a metric is central to threat detection.

A low priority was placed on measuring several behaviors. For example, though looking at threats (i) may be informative, use of an eye-tracking system would present a current technical challenge; however, the use of eye-tracking should be explored in future research. Some visual search measures can be accessed via a cued detection task where changes appear in locations consistent versus inconsistent with threats. Though experts may know the proper action to take for different threats (e), this investigation has focused primarily on steps leading to detection, and not those following detection. The reasoning and decision process regarding taking action versus investigating more deeply (f) is probably closely tied to the dangers of a particular situation, and the process of determining whether to ignore a threat, investigate a threat, or alert others about a threat could be difficult to remove from the context of the decision.

Table 7.

Metrics for Assessing Behaviors Associated with Expertise in the Threat Detection Loop

Measureable Behavior	Metrics	Priority
a. Encoding detail	SA Level 1 to 3	Medium
b. Threat vs. Non-threat decision	P(c), d', and RT for binary object classification task	Medium
c. Adapt selectivity	Signal detection theory (SDT) bias for noisy classification in response to feedback	Medium
d. Incorporate priors and causal theory	SDT bias and sensitivity for identifying threatening situations based on background stories	High
e. Identify appropriate course of action (COA)	Percentage of forced-choice COAs judged appropriate by subject matter experts (SME)	Low
f. Balance decision with info gathering	Amount of information needed to make a response, Prioritized threat assessment	Low, High
g. Ability to detect change or anomaly	Change and anomaly detection time; accuracy	High
h. Causal reasoning	Analytic coherence of causal story about potential threat	High
i. Looking at threats	Eye tracking distributions, Response time (RT) and accuracy for cued detection tasks	Low, High

Several of the metrics are of medium priority because of the potential difficulty of developing stimuli. Through a cost-benefit analysis, materials were developed that would provide the most return for cost. For example, measuring encoding detail (a) in terms of situation awareness would require developing a set of stimuli (images or video) that could not be reused on different trials to avoid learning effects. In this case, we assumed the return on cost would be small. Other metrics were given a medium priority because they were prioritized to be less important factors in expert threat detection. A large body of research shows the ability to adapt decisions about uncertain stimuli (c) in perceptual decision tasks (cf., Mueller & Weidemann; Weidemann & Mueller, 2008) and it may be more important to show ways in which detection sensitivity changes with expertise, rather than detection bias.

Several metrics were considered a high priority for experimental testing. These included ways in which high-level reasoning and information influences the search and the decision problem. For instance, how background knowledge about the way a threat might present itself could alter search strategies and detection abilities could provide useful information (d). This background knowledge includes an understanding of terrain features and intelligence information

consistent with threat, as well as causal reasoning about the process leading up to threatening situations. Soldiers can verbalize causal reasoning (h) which assists in determining Soldiers' underlying mental models. To measure the influence of these factors on visual search and attention, we tracked expert response time and recorded their ability to detect changes (i) that were consistent and inconsistent with expert knowledge. Further research incorporated change and anomaly detection (g) that was useful for simulating a more dynamic environment. These measures provided evidence to support the primary components of the threat detection loop.

Phase III: Preliminary Experiment

To determine if the stimuli, exercises, and metrics developed for the future research would support the primary objective of testing the expert model of threat detection, a preliminary experiment was conducted in Phase III. The methods developed for Phase III built upon the previous methods used in Phases I and II. The imagery analysis exercise contained dynamic threat monitoring/search, threat prioritization, and causal reasoning exercises. During interviews, Soldiers gave detailed threat analysis of several photos by constructing a story around each photo and providing explanations of potential threats they identified in the photos based on their experiences. This protocol was developed based on previous research in Phases I and II in order to test the proposed model and gather feedback from experienced threat detectors. Because of inclement weather, which limited the availability of Soldiers, results on the computer exercises are not reported. Rather, the method used in Phase III is described in Appendix M. Primary results from the interviews are reported here because Soldiers provided substantive insight about threat detection during their discussions.

Phase III: Interview Results

The interview recordings were classified into pre-determined categories, such as types of threats, threat cues, strategies for threat detection, and threat detection tasks, skills, challenges, and solutions.

The interviews provided information about the cues that Soldiers attend to in each photo and why they attend to those cues. Soldiers chose from a set of photos (Appendix N) the photos that reminded them of situations they had been in previously that they perceived as dangerous or threatening. They then discussed what was threatening about the scene in the photo, why it was threatening, and how to reduce the threat. Three of the four Soldiers choose to discuss the following photo (Figure 8). Soldiers expressed concern about threats related to the people in the photos and to the infrastructure (building, roads, etc.).



Photo for Threat Detection Discussion (Photo D, Appendix N).

Cues about human threat.

- The men on bicycles: The enemy fills them up with dynamite, “most of the guys who blow themselves up, will blow themselves up on a bike.” Another Soldier stated, “The bikes would be a concern and he's got a heavy coat on. He could hide an IED under it.”
- Need to see people's faces: Important to detect concern among the people in the area, “if they looked concerned, I'd be concerned.” They stated that indicators are behaviors such as frowning, standing in a defensive posture, and hands near weapons.
- Persons of most concern (man standing in front of the guard stand): “I can't see his hands and it looks like he has an argumentative stance. Next person of concern is by the bus walking towards us because he's coming into the sector as I'm approaching. I'd assume people would usually be leaving.” A second Soldier shared this opinion but tempered it based on the guard's stance, “He's my main concern. It looks like he's the owner of this vehicle, it might be a VBIED. However these guys (guards) are standing at ease, so the person may not be that bad.”
- Guards: Their behavior indicates that there is no immediate threat, “These people (guards) look really relaxed, so this doesn't ring out much.”

Cues about threats as a function of terrain.

- Sniper access areas: The biggest concern was all the windows surrounding this location and the potential threat from snipers who have easy access and a clear view of the area.
 - “This checkpoint is bad, period, because they can look at you from up [here]. You can have a trigger guy up [here] anywhere.
 - “They can have RPGs (rocket propelled grenades) from up [here]...that's a perfect lookout. In case the guy on the ground changes his mind, there's another trigger person.”
 - “There are a lot of places to hide up there... miserable time trying to see where a sniper is.”
- Vehicles: Soldiers were concerned about the car and less concerned about the bus:
 - “Two vehicles parked here is dangerous... if we went by and saw these two vehicles we'd be extra cautious.”
 - “The bus pulled over on side of the road looks like it's past the road. Maybe someone is living in it. Not sure if it's working or not.”
 - “If the bus was accelerating unreasonably fast. Nothing that size can move too fast, but to catch up and engage a convoy it would have to, so that would spark worry.”

Beyond pointing out threat cues, Soldiers provided hypothetical scenarios based on the information in the photo:

- “This guy (standing outside guard booth) might be their friend but [the enemy] has his family. He parks his car here, they may think he's their friend and he does it every day...he walks away and blows everybody up.”
- “If we came up on a deserted checkpoint and it wasn't manned, I'd call it in and lengthen out the convoy. I'd worry about a command-detonated wire placed on the side of the road. If it's a normally controlled area, someone would seize the opportunity that it's unmanned. I would watch the bluff and watch the buildings.”

Soldiers also explained the types of actions they would take if they came upon the scene in the photo:

- “There's not much I can do with that (vehicles and people) except direct the gunner's attention to stay trained on the yellow taxi-cab looking object. We'd probably slow down to ascertain what they're doing, if they are there to do harm. I'd call it up to the battlespace owner and have them come down and see what they can do to engage.”

- “It's pretty open, so depending on what's on the other side of the frame here I'd probably orient away from the building, change lanes and go across, even if that is [against] the directional flow of traffic.”

In addition to discussing cues to human and infrastructure threats, Soldiers discussed cues in the terrain (landscape, vegetation, hills, etc). For instance, in the following photo (Figure 9), Soldiers were concerned that the terrain around the work site allowed the enemy to stage an ambush or an IED attack. They explained that this point of the road is a chokepoint and the curve of the road obstructs their view.



Photo for Threat Detection Discussion (Photo G, Appendix N).

Soldiers were also concerned about some of the people in the photo. Of note is that both Soldiers who commented on this photo directed their attention to the man in the red hat and the other man crouching next to him (indicated by the arrow). They stated that these two men seem to be hiding, and unlike the others, they are not smiling, one is looking at (watching) the individual taking the picture and one is looking at the other workers. According to the Soldiers, this could indicate that these two men are in charge while the others serve as a distraction. These men could be planting an IED or concealing a weapon.

Top threat indicators across photos.

- Terrain and Infrastructure: open spaces, single lane roads, dense vegetation, rock piles, debris, ditches on the sides of the road, checkpoints, intersections, stone or rock walls, windows, high-rise buildings, broken asphalt, abandoned containers.
- Human: Looks of concern, aggressive or argumentative stance, looking away from troops, no identifiable purpose for being in the area, people seemingly out of place, talking on a cell phone, walking toward the troops, blocking troop movement, observing troop movement.

Many of the human threat indicators are actions that non-threatening individuals might make such as talking on a cell phone and observing troop movement. The challenge for Soldiers is to determine when to read these everyday activities as threats. It takes a combination of cues and situational elements to change observations of normal behavior into judgments of threats. For instance, in Figure 9, Soldiers stated the men pushing wheelbarrows were likely construction workers for American contractors, rather than a threat. Evidence of this includes the large number of workers, the fact that they are well dressed and the wheelbarrows are clean, and that they are showing their faces. One Soldier explained that these men could be using their work as a cover for an attack, or they may be locals working legitimately. These workers may know the two men crouching down are outsiders but they are afraid to say anything.

The exercises Soldiers engaged in during this phase focused on the primary processes, dynamic threat monitoring, threat search/prioritization, and causal reasoning. Though there were low participant rates during the preliminary experiment, feedback was gathered about the accuracy and relevance of all research materials. Discussions with Soldiers provided insight into their interpretation of the threats in the photos along with their reasoning about why these threats are important, the degree to which the threats are likely, and how they would respond to similar threats based on their experiences. Those findings, as well as feedback from the Soldiers about the exercises, indicate that the materials developed would provide a good test of threat detection skill.

Future Research

Findings from the research presented in this report will form the basis of further experimentation and development of a training exemplar. The questionnaire responses and the Soldier descriptions of threat types and threat cues during the interviews will inform future exercises by providing direction on how to modify the research stimuli. Based on the Expert Threat Detection Model and results from the preliminary experimentation, threat detection exercises will be modified and, stimuli selected for use in further research. The forthcoming research will assist in evaluating the current model of threat detection, which includes assessing the key processes of visual threat detection. Thus, the next phase of research will provide evidence for or against the identified processes of visual threat detection: *dynamic threat monitoring, threat prioritization, and causal reasoning*.

Summary and Conclusions

The information gained from a focused literature review, in-depth interviews, and computer-based exercises, provided a comprehensive perspective about the perceptual and cognitive processes most relevant for visual threat detection in an operational setting. Likewise, the experience and knowledge gathered from Soldiers and civilian police officers provided necessary information about the threat detection processes that were selected to be investigated more thoroughly in this research. The primary processes were determined to be, *dynamic threat monitoring*, *prioritizing threat cues*, and developing *causal inferences* about potential threats.

The knowledge gathered from Soldiers and police officers based on their experiences illustrated the randomness that is present in operational settings. Randomness seems to stem from the noise embedded in that visual environment and the effects are exacerbated by rare or inconsistent exposure to threat events. Soldiers and police officers reported that such randomness makes forming a coherent mental picture of the environment challenging, particularly if they need that mental picture to predict potential events in their surroundings.

Empirical research was leveraged to demonstrate that visual threat detection is a complex process involving the endogenous capacities of human observers whom operating in dynamic operational settings. Human observers utilize innate and adept skills to perform visual threat detection, but they may also be affected by potential information processing biases. Skills and biases can both exert influence on the overall ability to detect threats. However, as expertise develops through experience, biases become less influential. As shown in this report, purposefully examining specific perceptual decision-making processes has led to an increased understanding of how Soldiers visually detect and reason about threats in an operational environment. This understanding led to development of a theoretical model and the accompanying measures and metrics necessary to test the contentions of that model in future research.

The model of expert threat detection referred to as the threat detection loop, consists of several processes demonstrating that Soldiers hone skills as they attain experience and knowledge. Elaborate and in-depth responses gathered from operationally experienced Soldiers demonstrates these processes. The threat detection loop stems from the Recognition-Primed Decision model, which incorporates the notion of revising/updating one's visual threat detection perspective based on newly acquired information. Based on responses from Soldiers in interviews and on computer exercises, the processes determined most important for visual threat detection include *dynamic threat monitoring*, *threat prioritization*, and *causal reasoning*. As Soldiers become more proficient in their performance of the required skills, they are better able to detect, evaluate, and defeat a variety of threats in the visual environment. Achieving the overarching competency of threat detection allows Soldiers to comprehend, control, and manipulate the visual space, including any potential threats, while understanding their role and influence within that visual space.

References

- Ayton, P., Hunt, A. J., & Wright, G. (1989). Psychological conceptions of randomness. *Journal of Behavioral Decision Making*, 2, 221-238.
- Boyd, J. (1987). *A discourse on winning and losing*. (Document No. M-U 43947). Maxwell Air Force Base, AL: Air University Library
- Cole, G. F., & Smith, C. E. (2008). *Criminal Justice in America* (5th ed.). Belmont, CA: Thomson Wadsworth.
- Cooper, G., Tindall-Ford, S., Chandler, P., & Sweller, J. (2001). Learning by imagining. *Journal of Experimental Psychology: Applied*, 7, 68-82.
- Coram, R. (2004). *Boyd: The fighter pilot who changed the art of war*. New York: Little, Brown, & Company.
- Dreyfus, H. L., & Dreyfus, S. E. (1986). *Mind over machine: The power of human intuition and expertise in the era of the computer*. New York: The Free Press.
- Ericsson, K. A., & Charness, N. (1994). Expert performance. *American Psychologist*, 49, 725–747.
- Fama, E. F. (1970). Efficient capital markets: A review of theory and empirical work. *Journal of Finance*, 25, 383–417.
- Flin, R. (1996). *Sitting in the hot seat*. West Sussex, England: John Wiley and Sons, Ltd.
- Ginns, P. (2002). *When imagining instructions is effective*. Unpublished doctoral dissertation, University of New South Wales.
- Ginns, P. (2005). *Imagining instructions: A role for mental practice in higher education*. Unpublished document. University of Sydney. Australia, Sydney.
- Goodrich, M. A., Sterling, W. C., & Boer, E. R. (2000). Satisficing revisited. *Minds and Machines*, 10, 79–110.
- Green, C. S., & Bavelier, D. (2003, May). Action video game modifies visual selective attention. *Nature*, 423, 534-537.
- Green, D. M., & Swets, J. A. (1966). *Signal detection theory and psychophysics*. New York: Wiley.
- Helmuth, L. (2002, April 18). Video games score high for attention. *ScienceNOW*, 418, 3.

- Jerome, C. J. (2006). *Orienting of visual-spatial attention with augmented reality: Effects of spatial and non-spatial multi-modal cues*. (Technical Report 1215). Arlington, VA: U.S. Army Research Institute for the Behavioral and Social Sciences.
- Kahneman, D., & Klein, G. (2009). Conditions for intuitive expertise: failure to disagree. *American Psychologist*, 64, 515-526.
- Klein, G. (1997). The recognition-primed decision (RPD) model: Looking back, looking forward. In C. E. Zsombok & G. Klein (Eds.), *Naturalistic decision making* (pp. 285-292). Mahwah, NJ: Lawrence Erlbaum Associates, Inc.
- Klein, G. (1998). *Sources of Power*. Cambridge, MA: MIT Press.
- Klein, G. A., Calderwood, R., & Clinton-Cirocco, A. (1986). *Rapid decision making on the fire ground*. Proceedings of the Human Factors Society, 30th Annual Meeting (Vol. 1, pp. 576-580). Dayton OH: Human Factors Society.
- Kowalski-Trakofler, K., & Barrett, E. A. (2003). The concept of degraded images applied to hazard recognition training in mining for reduction of lost-time injuries. *Journal of Safety Research*, 34, 515-525.
- Lopes, L. L. (1982). Doing the impossible: A note on induction and the experience of randomness. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 8, 626-636.
- Markowitz, H. M. (1952). Portfolio selection. *Journal of Finance*, 7, 77-91.
- Mueller, S. T. (2009). A Bayesian recognitional decision model. *Journal of Cognitive Engineering and Decision Making*, 3, 111-130.
- Mueller, S. T., & Weidemann, C. T. (2008). Decision noise: An explanation for observed violations of signal detection theory. *Psychonomic Bulletin and Review*, 15, 465-494.
- Murphy, J. S. (2010). *Identifying experts in the detection of improvised explosive devices (IED2)*. (Technical Report 1269). Arlington, VA: U.S. Army Research Institute for the Behavioral and Social Sciences.
- Phillips, J. K., Klein, G., & Sieck, W. R. (2004). Expertise in judgment and decision making: A case for training intuitive decision skills. In D. J. Koehler & N. Harvey (Eds.), *Blackwell handbook of judgment and decision making* (pp. 297-315). Victoria, Australia: Blackwell Publishing.
- Salas E., & Klein, G. (Eds.) (2001). *Linking expertise and naturalistic decision making*. Mahwah, NJ: Lawrence Erlbaum Associates.

- Singer, M. J., Kring, P. P., & Hamilton, R. M. (2006). *Instructional Features for Training in Virtual Environments*. (Technical Report 1184). Arlington, VA: U.S. Army Research Institute for the Behavioral and Social Sciences.
- Staszewski, J. J. (1999). Information processing analysis of human land mine detection skill. In V. T. Broach, A. C. Dubey, R. E. Dugan, & J. Harvey, (Eds.), *Detection and Remediation Technologies for Mines and Minelike Targets IV*, Proceedings of the SPIE Conference, 3710, 766-777.
- Taleb, N. N. (2007). *The black swan*. New York: Random House.
- Tolcott, M. A., Marvin, F. F., & Bresnick, T. A. (1996). Situation assessment and hypothesis testing in an evolving situation. (Research Note 96-34). Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Sciences.
- U.S. Department of Army (2006). *Counterinsurgency*. (Field Manual 3-24). Washington DC: Author.
- U.S. Department of Army (2008). *Operations*. (Field Manual 3-0). Washington DC: Author.
- U.S. Department of Army. (2008). *Combined Arms Improvised Explosive Device Defeat Operations*. (Field Manual 3-90.119). Washington, DC: Author.
- U.S. Department of Army (2011). *Training Units and Developing Leaders for Full Spectrum Operations*. (Field Manual 7-0). Washington DC: Author.
- Vowels, C. L. (2010). *Asymmetric attention: Visualizing the uncertain threat*. (Research Report 1916). Arlington, VA: U.S. Army Research Institute for the Behavioral and Social Sciences.
- Weidemann, C. T., & Mueller, S. T. (2008). Decision noise may mask criterion shifts: Reply to Balakrishnan and MacDonald (2008). *Psychonomic Bulletin and Review*, 15, 1031-1034.
- Zimmerman, L. A., Mueller, S. T., Daniels, J., & Vowels, C. L. (2012). *Developing training exemplars for the requisite components of visual threat detection*. (Technical Report 1322). Fort Belvoir, VA: U.S. Army Research Institute for the Behavioral and Social Sciences.
- Zimmerman, L. A., Mueller, S. T., & Grover, J. (2009). *Attention: Threat Detection in the COE Literature Review*. Unpublished manuscript.

Appendix A

Acronyms

ANOVA	Analysis of Variance
AO	Areas of Operations
COA	Course of Action
COR	Contracting Officer Representative
CPT	Captain
DoD	Department of Defense
FM	Field Manual
IED	Improvised Explosive Device
LT	Lieutenant
MAJ	Major
MOS	Military Occupational Specialty
NCO	Non-commissioned Officer
NVG	Night Vision Goggles
OE	Operational Environment
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OIL	Observations, Insights, and Lessons Learned
OODA	Observe, Orient, Decide, and Act
PBIED	Person-Borne Improvised Explosive Device
PEBL	Psychology Experiment Building Language
RPD	Recognition-Primed Decision (model)
RPG	Rocket propelled grenades
ROE	Rules of Engagement
RT	Response time
SDT	Signal Detection Theory
SGT	Sergeant
SME	Subject Matter Expert
SOP	Standard Operating Procedures
TTP	Tactics, Techniques, and Procedures

UAV	Unmanned Aerial Vehicles
USAF	United States Air Force
VBIED	Vehicle-Borne Improvised Explosive Device
WMD	Weapons of Mass Destruction

Appendix B

Demographic Questionnaire – Phase I (1a), Session 1 & 2; Phase II; and Phase III

Time in Service: _____

Current Rank: _____

Time in Current Rank (in months): _____

Current MOS: _____

Age: _____

Previous Deployments

Location	Unit deployed with	Length of deployment mm/yyyy to mm/yyyy	Rank during deployment	MOS & duties during deployment

Appendix C

Threat Questionnaire – Phase I (1a), Session 2; Phase II, and Phase III

Please rate each question on the 5-point scales below:

1. When trying to detect threats in current operating environments, how concerned are you about each of the threats listed below?

Dangerous or malicious persons (PBIEDs or distributors of other weapons, intel gatherers)

Not at all concerned 1 ----- 2 ----- 3 ----- 4----- 5 Extremely concerned

Roadside IEDs

Not at all concerned 1 ----- 2 ----- 3 ----- 4----- 5 Extremely concerned

Vehicle threats (VBIEDs, vehicle intrusions into secure locations)

Not at all concerned 1 ----- 2 ----- 3 ----- 4----- 5 Extremely concerned

WMDs in urban settings

Not at all concerned 1 ----- 2 ----- 3 ----- 4----- 5 Extremely concerned

WMDs in non-urban settings

Not at all concerned 1 ----- 2 ----- 3 ----- 4----- 5 Extremely concerned

2. Rate how difficult it is to detect each of these threats

Dangerous or malicious persons (PBIEDs or distributors of other weapons, intel gatherers)

Not at all difficult 1 ----- 2 ----- 3 ----- 4----- 5 Extremely difficult

Roadside IEDs

Not at all difficult 1 ----- 2 ----- 3 ----- 4----- 5 Extremely difficult

Vehicle threats (VBIEDs, vehicle intrusions into secure locations)

Not at all difficult 1 ----- 2 ----- 3 ----- 4----- 5 Extremely difficult

WMDs in urban settings

Not at all difficult 1 ----- 2 ----- 3 ----- 4----- 5 Extremely difficult

WMDs in non-urban settings

Not at all difficult 1 ----- 2 ----- 3 ----- 4----- 5 Extremely difficult

2a. Relative to the others, which threat is most difficult to detect? Why?

2b. Describe the cues/indicators that would indicate this threat is present:

Rate how difficult it is to detect the following indicators of a threat

Non-verbal behavior (behaviors, movements, facial expressions) that indicates malicious intent
Not at all difficult 1 ----- 2 ----- 3 ----- 4----- 5 Extremely difficult

Verbal behavior (tone of voice, voice volume, content of conversation) that indicates malicious intent
Not at all difficult 1 ----- 2 ----- 3 ----- 4----- 5 Extremely difficult

Roadside anomalies (upturned dirt, packages, out-of-place vegetation, etc.) that indicate roadside explosives
Not at all difficult 1 ----- 2 ----- 3 ----- 4----- 5 Extremely difficult

Roadside anomalies (upturned dirt, packages, out-of-place vegetation, etc.) that indicate enemy presence (attack or surveillance)
Not at all difficult 1 ----- 2 ----- 3 ----- 4----- 5 Extremely difficult

Vehicle behavior (weighted down trunk, erratic driving, etc.) that indicate vehicle attack
Not at all difficult 1 ----- 2 ----- 3 ----- 4----- 5 Extremely difficult

Vehicle behavior (weighted down trunk, erratic driving, etc.) that indicate smuggling (weapons, persons, etc.)
Not at all difficult 1 ----- 2 ----- 3 ----- 4----- 5 Extremely difficult

Items in buildings (explosive materials, Intel) that indicate terrorist activity
Not at all difficult 1 ----- 2 ----- 3 ----- 4----- 5 Extremely difficult

Urban street anomalies (nobody around, moving curtains, suspicious packages, etc.) that indicate terrorist activity
Not at all difficult 1 ----- 2 ----- 3 ----- 4----- 5 Extremely difficult

Appendix D

Interview Protocol – Phase I (1a), Session 1 and 2 (enlisted)

RE: Interview Protocol

TITLE: Attention: Threat Detection in the COE

All questions will involve your knowledge and experience involving dismounted patrols and/or convoy operations, especially involving your ability to detect visual threats and/or visual indicators of potential threats. Your responses will be recorded in audio and written format, but you have the right to have any of your responses withheld from being recorded. Questions are not meant to be evaluative.

1. What is your experience conducting convoy operations and/or dismounted patrols?
2. What training did you receive on detecting visual threats *before* deployment?
3. What training did you receive on detecting visual threats *during* deployment?
4. What training have you received on detecting visual threats *after* you deployed?
5. Was training for detecting visual threats coupled or piggybacked with other types of training?
6. What training would you have liked to have received that you never got or didn't get enough of to feel comfortable executing the threat detection tasks you were required to perform?
7. What was the primary purpose of your patrols or the most common purposes?
8. Did you ever perform patrols where your primary task was to locate IEDs or similar threats?
9. Were IED threats independent or were they coupled with other threats (more IEDs, small arms fire, etc.)? Were you trained to respond to such threats?
10. Did threats change across time in your AO? If so, how? Were you prepared? Why/why not?
11. What instruments or tools did you have available to help train "new" and "old" Soldiers on the potential threats in your AO?

12.	If you could do something(s) differently to assist in visual threat detection, what would you do? -At the, individual, squad, platoon, company, etc.
13.	Were there situations where initial non-lethal cues became indicators of later lethal threats?
14.	Did you rely on certain personnel the most to detect visual threats? If so, what capability did those personnel possess that was so valuable?
15.	What equipment and tools did you have available to deal with visual threats? Did it help?
16.	What was the most effective means for detecting IED threats, snipers, and like threats?
17.	If training were developed for visual threat detection, what would be most easily utilized by you, both individually and collectively? PowerPoint? Simulations? (Video) Games? Lanes training? Combination?
18.	If comfortable discussing, could you provide an instance where a threat was not detected and led to a negative outcome? What could have prevented it (if anything)? What training was missing?
19.	Could you provide an instance where a threat was detected and led to a positive outcome? What things went right and why? Did you adapt to the situation or did you rely on training you had received or both?
20.	Did you train for visual threats individually, collectively or both?
21.	When on task for a long period, what things, if any, do you do to stay attentive and alert? Did you receive training on vigilance (i.e., staying alert)?
The next set of questions will focus on three particular sections involving the visual detection of threats, just different contexts: human-human interaction, human-computer interaction, and human-terrain interaction.	
Human-human interaction (such as, interpersonal engagements)	
1.	What training have you received on interpersonal communication, such as working with an interpreter to communicate with a foreign counterpart and/or local-national?
2.	Did you receive training on detecting threats or potential warning cues by paying attention to an individual's verbal and/or non-verbal behavior? Were there certain indicators you would watch for while observing someone's behavior?

3. Did you receive training on visually scanning your environment to detect threats?
4. What particular training was helpful? Which was not?
5. What would have been beneficial for you in terms of <i>human-human</i> training, before you deployed or deploy again?
Human-computer interaction (such as, viewing a computer monitor for warning)
1. What training have you received on monitoring (computer) displays for indication of threat?
2. Did you receive training on detecting threats or potential warning cues for certain displays or systems?
3. What particular training was helpful? Which was not?
4. What would have been beneficial for you in terms of <i>human-computer</i> training, before you deployed or deploy again?
Human-terrain interaction (such as, viewing the landscape for indicators of IEDs, etc.)
1. What training have you received on monitoring the terrain for indication of threat?
2. Did you receive training on detecting threats or potential warning cues for certain terrain types or for certain threats that could be encountered on patrols?
3. What particular training was helpful? Which was not?
4. What would have been beneficial for you in terms of <i>human-terrain</i> training, before you deployed or deploy again?

Appendix E

Short-answer Protocol – Phase I (1a) – Session 2 (officers)

RE: Interview Protocol

TITLE: Attention: Threat Detection in the COE

All questions will involve your knowledge and experience involving dismounted patrols and/or convoy operations, especially involving your ability to detect visual threats and/or visual indicators of potential threats. Your responses will be recorded in written format, but you have the right to have any of your responses withheld from being recorded.

Questions are not meant to be evaluative.

Threats

1. ***What is your experience conducting convoy operations and/or dismounted patrols?**

**Spaces for responses are reduced to conserve space in the current document.*

2. **What were the most common purposes of your patrols?**

3. **What threats were you most concerned about while on patrol?**

4. **How did the types of threats you encountered in your AO change over time? Were you prepared? Why/why not?**

5. **Please describe an incident where you detected a threat and acted upon it. Did the threat turn out to be a valid threat? Were you successful at mitigating the threat?**

6. **Please describe the typical cues that indicate the presence of a threat. Describe the type of information you need before you reduce the risk surrounding the threat.**

7. **Describe the ways in which your ability to detect threats has changed with experience. Provide examples.**

8. **How does the manner in which you scan for, detect, and react to threats change when you are working in a team vs. alone?**

9. **What do you think aided you most, memory of an area (or route) or paying attention to details? Why?**

Technology

10. **What instruments/tools/technology do you use to aid in threat detection?**

11. **What types of instruments/tools/technology would you like to have to assist in threat detection (real or imagined)?**

Training	
12.	Describe training you have received that helps you detect threats? Did you receive this training before, during, or after deployment?
13.	In hindsight, what type of training would have helped you better detect threats?
14.	What type of training was, or could be, effective in threat detection during human-human interactions (i.e., interpersonal interactions)?
15.	What type of training was, or could be, effective in threat detection during human-computer interactions (i.e., computer monitoring, warning systems)?
16.	What type of training was, or could be, effective in threat detection during human-terrain interactions (i.e., landscapes, urban settings)?
17.	What type of threat detection training format would be most useful to you - PowerPoint? Computer-based simulations (i.e., video games, scenario-based learning)? Live simulations? Lanes training? Combination?
18.	If you had to train other Soldiers about threat detection, what key factors would you make sure you included (what things would you want Soldiers to know before they deployed)?
19.	What instruments or tools did you have available to help train “new” and “old” Soldiers on the potential threats in your AO?

Any further comments you have would be greatly appreciated. Thank you.

Appendix F

Summary of ride-along activities – Phase I (1b)

Officer 1

Officer 1 had the least amount of experience (2 years). She interacted with the community a great deal during the patrol. She knew the names of many of the people who “hang out” in the area, including drug dealers, drug users, gang members, the homeless and unemployed, and merchants. She nurtured these relationships to gain respect and to gather intelligence about future and past criminal activity.

Officer insight. Officer 1 stated “Police are just glorified babysitters.”

Patrol activities. The officer drove around, stopping often to speak with people and ask questions about recent activities. She said people tend to give her information about serious crimes, such as shootings, rather than information about drug dealing. During the ride-along, she was searching for information on a string of burglaries in the area and trying to enlist the help of community members to stop the burglars. She scanned the environment for any signs of trouble or criminal behavior.

She observed drug dealer patterns and was aware that the dealers know police patterns (e.g., shift change). For instance, a large group of people was observed walking quickly away (in different directions) from a known drug dealer’s house. Officer 1 stated that earlier in the day they had stopped a dealer who was giving out “freebees” (free drugs to get addicts hooked on their products). She knew that when one dealer gives away free drugs, the others often do the same. Driving by this dealer’s house had stopped the “freebee” and an increased police presence around the house would stop activity for a while. Unfortunately, this action was only a temporary fix that will not stop the drug problem. Police often cannot arrest the drug dealers because the dealers do not keep enough drugs in their homes to warrant an arrest. The police need to find where they stash the drugs and connect the drugs to the dealer to make an arrest.

Calls-for-Service. The only call-for-service related to threat detection was a call to a house burglary in progress. We arrived at an abandoned house with backup. The officers drew their weapons and went in to search the house (the experimenter stayed outside until the officers cleared the house). The officers described the search: They could hear someone in the house and slowly searched each room. They passed a shut basement door that they left shut while an officer stood guard in case anyone came out. As the officers went upstairs, the smell indicated that a homeless person was inside. They called out and the homeless person responded and came out with his hands up. Searching houses is a complex task with a great deal of uncertainty that officers must manage as they weigh the risks of going in one direction versus another, or choosing to look in one direction first. They often have little or no information to guide these decisions and must rely on their quick assessment of an unfamiliar environment and their experiences.

Threat detection activities. Officer 1 discussed threat cues in her patrol area and stated that she mostly relies on non-verbal cues to detect threats, including subject movements such as

walking away from officers and refusing to look at officers. In her opinion, most people act defiant rather than nervous when they are culpable. Some act overly friendly or helpful as they try to divert the police away from their own (or their associates) criminal activity. Here are a few observations made by Officer 1:

- When drug-dealing activity is going on in an area that the officer is close to, someone will stop the officer and distract them by acting very friendly and talkative.
- Drug dealers place bicycles and trashcans containing rocks in the middle of alleys so police cars cannot get through.
- We called out to a man on a bicycle and the man stopped to talk to us. Officer 1 stated that he was not holding drugs because he stopped. If he were holding he would have kept riding.
- The norm in the neighborhood is drug dealing and loitering. It is difficult to detect threats like weapons from this activity. Officer 1 claimed that she mostly relies on body language and gut feeling.

Officer 2

Officer 2 had 9 years experience and on the night of the patrol, he was the acting Sergeant (SGT) for this shift. This meant he would travel throughout the entire district rather than staying in one sector. All other officers patrol one sector within the district. Officer 2 liked to focus on stolen vehicles during his patrol. He would run the plates on suspicious vehicles, and if stolen, he would conduct surveillance until the thief showed up to drive the car and then he would make an arrest and return the car.

Officer insight. Officer 2 said that policing is largely about common sense. He stated that it is important for police to remember that criminals are often very clever and creative. Police often assume they are dumb, but the “bad guys” spend much of their time figuring out ways to outsmart the police. And, unfortunately, these criminals are often successful.

Patrol activities. The officer drove around to check on officers while they were handling calls. Officer 2 knew several local merchants and residents in the area and stopped to ask how they were doing and how things were in the area. As the officer patrolled the area, a man turned quickly down an alley after he saw us. Officer 2 turned around to see what the man was up to, but he had disappeared by the time we got to where he was. The officer remained on the lookout for him during the remainder of the shift.

The officer drove past a man standing in a front yard. Officer 2 was suspicious and backed the car up to talk to the man. When we returned, the man was “knocking” on the front door. Officer 2 stated that it was common for people to act as if they belong at a house by pretending to knock on the front door. When Officer 2 questioned the man, the man responded with hostility. Officer 2 put his hand on his gun, unsnapped the holster, and asked the man for identification. The man became increasingly belligerent and walked toward Officer 2. Officer 2 pulled his weapon but did not raise it as he told the man to get back. The residents of the house came out and said they knew the man but they had not invited him into the yard or house. Officer 2 searched the man, did not find any weapons or drugs, and told the man to leave the area. The officer did not know why the man was hostile, saying that he “probably just hates

cops.” This type of situation provides an illustration of how community climate and attitude can influence perceptions of threat. The man was not a threat but was hostile because of his general attitude. Because Officer 2 was aware of this general attitude, he did not overreact to the hostility that in other situations might have indicated a greater threat level and a call for greater use of force.

Calls-for-Service. Because Officer 2 was the acting Sergeant, he did not respond directly to calls for service. He would show up to calls to provide assistance if necessary. No calls dealt with threat detection.

Threat detection activities. Officer 2 was not nearly as active in detecting threats as was Officer 1. He explained that younger officers tend to be more vigilant and react to smaller threats and crime signals even though this expends a lot of wasted energy. He claimed that these newer officers know what to look for but often miss subtle things that indicate a real threat. In contrast, more experienced officers are usually more relaxed and tend to let things go that are not worth their attention. They know better what to look for in situations and tend to interpret things from gut feelings rather than reacting to every indicator. The other side of this is that experienced officers tend to get complacent and miss the indicators to serious threats, which can be dangerous or even deadly.

Officer 3

Officer 3 had 10 years experience. He exhibited the positive qualities of an experienced officer that Officer 2 described. He was observant but not hyper-vigilant. He responded to subtle activities in the environment rather than the common and obvious activities, such as drug dealing/purchasing and loitering. He had relationships with many community members and seemed well known and respected by the locals. He acted as a “police presence” by parking at strategic locations to stop and deter crime and to disrupt drug dealer business while he was there.

Officer insight. Officer 3 stated, “The neighborhood doesn’t want you (cops).” To overcome this, he said that officers must become familiar faces, be consistent in their presence, and be persistent in building relationships. He said, “it does not matter if they do not want you there, someone will talk,” claiming that there are always people in the community who do want officers there and they will eventually talk to familiar officers. He explained that a key strategy is to talk to kids, who are curious. Once the kids think, “he’s alright,” they will tell their parents who will come out and talk.

Patrol activities. Two patrol events provide good examples of expert threat detection in police patrol environments:

1. The officer drove by a group of four men standing in the driveway of an abandoned house across the street from a transportation station (busses, subway) and half a block from a bus stop. The men were not really standing together in a group but all were in the same driveway, looking across the street at the transportation station. Officer 3 noticed this as the officer drove by and turned around to investigate. When we returned, one man was driving away. The other three stated that they were waiting for the bus. Officer 3 drove away and called for backup. He said that the situation did not look right and he sensed one of the men had a gun. He said their stance

made him suspicious and concluded that because of where they were standing they were not waiting for a bus and yet they were not leaving the area.

We met three other officers a few blocks away from the bus stop and Officer 3 briefed them on his suspicions. The officers drove in three patrol cars back to the location. Two of the men tried to drive away when they saw us coming. We followed one man, who pulled over and let Officer 3 search him and his car. No weapons or drugs were found. The car had legal registration and insurance and the man had a valid driver's license. His driver's license indicated that he was from another part of town not close to this district. He did not provide a good reason why he was standing in the driveway looking at the transportation station and he did not provide any information about the other men. Officer 3 told him to leave the neighborhood and not return to the spot.

We went back to the other officers. The circumstances of the other man who tried to drive away were the same as the first man who was stopped. His driver's license indicated he lived in another part of town, different from the first driver. The third man ducked behind a van when he saw the officers arrive. He crouched down in a way that made the officer think he was pulling a weapon, so the officer drew his weapon. The man put his hands up and stood up. The officers searched the man and the van but did not find any weapons or drugs. This man also lived in a different part of town from the other two men.

Because the officers did not find any weapons or drugs, they surmised that the men might be drug deliverymen from their respective neighborhoods who were waiting for a drug delivery from their mutual supplier. Though this cannot be confirmed to be the correct assumption, but the behaviors of the men, the fact that they all had legally registered cars (thus, not waiting for the bus), and their diverse addresses led the officers to believe this is the most plausible explanation. The officers reported the incident and asked that undercover officers stakeout the area in hopes of catching the supplier.

2. The officer was driving through an intersection, glanced up the cross street, and viewed an old, beat up pick-up truck at an angle in the road. I thought the driver was parking. Officer 3 thought the truck looked suspicious, so we drove back around. We got there quickly but the truck was gone. As the officer continued on patrol, the truck crossed his path again. Officer 3 pulled the truck over. He noticed the temporary tags on the back window and thought it looked suspicious. The driver did not have vehicle insurance and his driver's license was suspended for failure to pay child support. Officer 3 owned several car dealerships and noticed immediately that the registration was a forgery. He also noticed several tools in the back of the truck that thieves often use to steal copper and fixtures from abandoned houses. Several of the houses where we first saw the truck had recently been broken into. Officer 3 took a second look at the temporary tag and realized it was also a forgery. The driver had created a tag on paper and glued it to the back of cardboard so it could stand in his back window. It was a good imitation, but because of Officer 3's dealership experience, he recognized that it was not real. Officer 3 had the truck towed away and issued the driver tickets for driving without a license or insurance in an unregistered vehicle (it was not reported stolen).

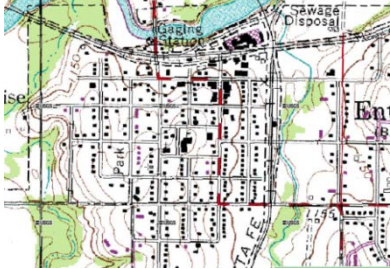









Calls-for-Service. No calls for service directly related to threat detection

Threat detection activities. Officer 3 detected threats in the two situations discussed above that more junior officers might have missed. The threats in these situations were not life threatening in the moment, but Officer 3's actions likely prevented further crime, at least for that day. He demonstrated the ability to react to subtle cues rather than blatant cues that officers have little influence over (i.e., drug dealers walking away from police). In each situation, something unknown caught Officer 3's attention and he let his gut feeling guide him back to the scene. Several cues were present that indicated the officer should continue to investigate, and the cumulative information confirmed for him that he was correct in this initial assessment.

Appendix G

Images for Imagery Analysis – Phase II

Enlarged versions of the images below were shown to participants in Phase II for annotation. At each point Soldiers selected, they judged the severity and likelihood of a threat on a 3-point scale, and provided a brief text description of the perceived threat.

Appendix H

Interview Protocol – Phase II

Interview Objective

Understand threat detection processes and abilities developed through training and experiences within the COE.

- Elicit recent threat detection experiences during mounted and dismounted urban patrols in OEF or OIF.
- Identify the critical components of threat detection.
- Identify the threat detection skills that develop with experience.

Part I

Briefly describe a particularly challenging MOUT patrol situation in which you successfully detected a threat. Describe the threat, what you noticed, and how you responded.

- *Alternatives:*
 - *Describe the main type of threat you look for while on patrol in urban environments. Did you ever need to respond to these threats? Which are the most difficult threats to detect and why?*
 - *Describe a time when you missed a threat. What were the consequences? What would you do different now?*
- Have the participant describe a situation uninterrupted.
- Work with the participant to create a timeline of the event, identifying key points of threat detection (attention, perceptions, threat cues, change detection, etc.), actions, and decisions.
- Ask probe questions to address key timeline elements.

Probe Questions

What was the most difficult threat detection challenge in this situation?

- What made this challenge difficult?
- What was your main objective in this situation?
- How did this challenge impact your ability to achieve your objective?
- What was your biggest concern in detecting this threat in this situation?
- Did you experience any similar challenges in other situations? If so, how did you manage it similarly/differently?

How did your combat experience influence your ability to detect and assess the threat in this situation?

- What threats were you looking for?
- Describe the moment you first noticed a potential threat.
 - What actions did you take to assess this threat?
- What did you notice (see, hear, etc.) in the environment that led you determine this was a real threat?

- Do you rely on these same cues in other situations or do attend to different cues based on each situation?

What is the first action you took when you realized this was a valid threat?

- What did you expect to happen when you took this action?
- Why do you think things happened the way you did/did not intend?
- What actions might a Soldier take that would lead to a better/worse outcome?
- What factors/cues/indicators would someone without experience or training in threat detection miss as he/she tried to detect threats in this situation?
- What do you know now, because of your experiences, that you wish you knew prior to military service?

Part II

Training needs

What type of threat detection training did you receive prior to and during deployment?

- Describe any specific threat detection training you have had.
- Describe any other training that you think helped you to detect threats.
- What have you learned from experience would be useful for other soldiers to learn in training?
- Describe anymore/different training you would like to see that addresses threat detection.
 - Describe any current training you think is particularly useful.
 - What types of training would you like to see developed?
 - E.g., scenario-based (live exercises or computer-based), classroom training, content added to existing courses, etc.

Describe any training you have had in the following areas:

- Interacting with locals (i.e., working with an interpreter, scanning a crowd)
- Managing systems/technology intended to help them detect and mitigate threats
- Basic skills such as scanning the terrain in both urban and rural settings
 - What type of training would be useful in these areas?

Appendix I

Screen Capture of Imagery Analysis Exercise – Phase II



- 1 I would not buy anything from this market that would be fed to anyone of any importance.
- 2 heavily clad people can be disguising weapons/ bombs
- 3 visibility / communication would be poor in the missile of the market
- 4 Potential PBIED; 'booby' traps, small arms
- 5 sorry, clicked here
- 6 Cannot identify any major threats in this photo
- 7 possible enemy
- 8 possible enemy
- 9 possible enemy
- 10 possible enemy
- 11 possible enemy
- 12 possible enemy
- 13 possible enemy
- 14 possible enemy
- 15 possible enemy
- 16 possible enemy
- 17 Possible IED in small carts
- 18 Possible suicide bombers throughout crowd
- 19 Possible placement of deep buried IED in fresh turned dirt
- 20 Good sniper position if no 360 degree security
- 21 I would watch for snipers on the building before I enter the market
- 22 while im walking though the market check out the ground to make sure it has
- 23 make sure i watch every personally to see if they mit have explosive
- 24 bulky garments can conceal suicide bomb
- 25 possible cache or led building shop
- 26 busy markets make great bombing targets due to large numbers of people
- 27 getting in too deep can cause a problem if locals are hostile
- 28 could house IED production
- 29 Great possibility of a suicide bomber./
- 30 Building could conceal a near-side ambush
- 31 Crowded space is an ideal location for a PBIED
- 32 Shopkeepers could sympathize with insurgency, call in our location and activity for a future attack
- 33 This man is wearing considerably more clothing than the other people in the market.
- 34 This narrow alley has direct fire and observation of the market stands.
- 35 If a unit frequents a market, the food can become a target for poisons
- 36 Possible choke points and ambush sites.
- 37 Baggy clothes, suicide vest
- 38 The market is fairly busy. Probably not much enem activity planned
- 39 caution for personal led
- 40 the enemy can and may be hiding behind any booth
- 41 with all the movement in the kJmarket it makes it hard to see down the road
- 42 could be an ambush with small arms fire.
- 43 led possible but too much population hangin around
- 44 at markets people may also lay out cover up explosives on the side of the road so people may think they are fruits or crops
- 45 explosives may be burried in the bottom of wheel barrow for delivery.
- 46 explosives may be covered up by bags
- 47 locals may be smuggling explosives un noticed
- 48 IED concealed in garage, less likely but could be very severe
- 49 different color dirt. maybe IED placed here
- 50 Alleys between bldgs allow rtes for attacks
- 51 closed up shops interesting in market...pos staging/prep area
- 52 notice the kind of conversation being carried, gestures, facial expressions
- 53 will the people stay and converse or will they leave
- 54 is there any movement, are they hiding firearms or any other weapons
- 55 enemy intel collector
- 56 SVIED
- 57 SVIED 9 walking towards me
- 58 Dark spot where you can observe and not be observed. Great spot for a trigger man
- 59 Whatever is behind that telephone poll is not a part of the natural surroundings
- 60 Break between buildings, lookout/sniper escape
- 61 Why are these shops closed, what does the owner know
- 62 What has this man been hauling
- 63 Threat of sniper hiding along some window or building.
- 64 Lots of unknown local nationals around that could kidnapp, suicide bomb or ggrande attackj.

Appendix J

Example Annotations from Imagery Analysis – Phase II

1. Crossing the tracks could pose a problem if the convoy is split by a train.
2. Area is more heavily populated than the rest of the map- could pose more threat.
3. To me the Flag on this bldg indicated an official building. I would avoid this building.
4. This is a congested area that I would take extra care in crossing. I would ensure my trucks were spread out.
5. Crossing the river would be the most dangerous part of the trip in my mind. You are exposed and have to escape route off of a bridge.
6. I would take this route because there is less population here.
7. Bridge crossing, potential IED.
8. Mosque; potential extremist activity, weapons cache.
9. Potential second story bldgs down both sides of street, potential attack position.
10. Railroad crossing; potential IED.
11. Major bridge crossing, potential IED, analyzed loc. For ambush.
12. General; routes outside town, fast moving convoys, hard to identify IED locations.
13. General; alleys/cross streets, no visibility, good ambush location.
14. Potential EFP Location.
15. Possible Ambush Sight/Could use EFP or IED to disrupt movement.
16. IED/EFP Location.
17. Main intersection possible point of contact.
18. Out of the way area, T intersection could be point of contact.
19. Bottle neck over water could be used for IED or EED.
20. Location of possible IEDs.
21. Location of trigger man.
22. Location for RPG team to hit convoy.
23. Whole stretch good place for a number of IEDs.
24. More RPG teams.
25. Possible location for VBIED.
26. Any kind of hill top overlooking the river.
27. Because once you start crossing there's only north or back south.
28. Because it looks over three intersection that the convoy turns.
29. Once they hit you on the bridge they can open up with anything.
30. Vehicle born IED could hit you coming from the north or east.
31. Could be a sniper over watching the intersection and bridge.
32. Sniper on the building over watching the intersection.
33. Same as number five but the car would either be moving from the west or south.
34. VBIED moving from the east could hit your convoy.
35. Could be explosive under the bridge or a kid or any body through a grenade.
36. Risk of small arms fire and IED.
37. Choke point risk for small arms fire from north side of river and sniper fire.
38. Risk of small arms fire, sniper fire and remote IEDs due to multistory buildings on east and west sides of street.
39. Risk of sniper fire from multistory building and lack of cover and concealment.

40. 3 way less escape routes.
41. Rail crossing prior to bridge limits escape and provides hide sites.
42. Intersection that could be used as a VBIED.
43. Choke point for IEDs.
44. Bridge locations for IED, causing a break within coalition forces.
45. Intersection that could be used to attack convoy with VBIED.
46. Intersection that could be used for IEDS / VBIEDS.
47. Three way intersection used to use VBIED.
48. Bldgs for a sniper.
49. Bridge that could hide an IED.
50. High likelihood of ambush or IED at the bridge chokepoint.
51. Major intersection, enemy knows we're likely to pass by.
52. Corner we'll have to slow down for, making us more vulnerable.
53. Wooded area w/ LOS to the intersection offers concealment for sniper or forward observer.
54. Buildings have LOS to the bridge, good place for sniper or FO, also has high speed evac route.
55. Bridges are likely targets for larger IEDs and offer the enemy a great view of my patrol.
56. This is a choke point with multiple enemy escape routes.
57. Enemy can observe my intended route with no question; the bridge.
58. Dense urban buildings offer the enemy ideal terrain for ambush.
59. Possible ambush and choke point site.
60. Good place to place an IED, can destroy bridge and trap team.
61. Possible IED.
62. Possible v-bed, IED, destruction of bridge.
63. Sniper fire from surrounding buildings.
64. The windows of this building and roof.
65. Possible IED first intersection into the town.
66. T-road intersection. possible ambush. nowhere to go.
67. Bridge could be rigged with explosives.
68. IED; rpg possible small arms attack from structures across the intersection.
69. Bridges rigged w/explosive.
70. Rpg small arms at pass patrols.
71. Rpg small arms attack from opposing structures.
72. Multiple angle ambush, large structures for enemy cover, multiple weapon choke point use
73. Light harassment when passing intersection, small arm, rpg, IED.
74. IED small arm rpg attack when patrol slows and crest any of the turns in the route.
75. Major intersection, possible for IEDs in the corners.
76. Soft shoulders might give no escape route and stream also causes a choke point.
77. High population and traffic will slow down mission and tall building may be good sniper hideouts.
78. Bridge creates great choke point and good ambush sector.
79. Dense bldgs, good view high traffic area.
80. Bridge could be rigged with explosives.
81. Excellent IED location. Has multiple observation posts with cover.
82. If this is overseas, a mosque...it is pretty much off limits and excellent place to stage attacks.

83. Intersection, IED.
84. Ambush point.
85. Enemy gathering point.
86. Possible ambush site, IED.
87. Dense urban area, possible ambush.
88. Possible IED, open main road.
89. South Bank bridge- an attack could occur after the friendly elements.
90. Small arms and sniper fire danger from built up areas, difficult to detect.
91. Choke point, not many avenues to maneuver out of once the bridge is crossed.
92. Natural choke point. The only way to maneuver is north or south.
93. Enemy can engage from the far bank of the river or from buildings within the town.
94. Enemy can take advantage of buildings to use as cover or for a top down attack.
95. Both sides of the bridge and side rails.
96. Ammonia discharge possible.
97. Park, open area that is not on the main path, IED heaven.
98. Religious center, hostiles could be very protective of this site.
99. Railways always have burms or cuts and overgrowth, IED/complex attack.
100. Waterway both sides channel you through town vs. fording.
101. Main avenue with turns, lookouts can signal around corners; side roads may be narrow.
102. Chokepoint for crossing forces. Far side ambush.
103. Possible ambush site due to main road curve.
104. IED ambush due to stream culvert.
105. Snipers in urban area.
106. Large cluster of buildings could be a market with possible VBIED, suicide vest, or grenade attack.

Appendix K

Imagery Analysis Word List – Phase II

A total of 2,928 word tokens were extracted from the text annotations (common 'stop' words were excluded, for a total of 276 distinct words). The raw frequencies of these words (with minor edits for spelling, and abbreviations, and word tense) were found. Then, the raw frequencies of these same words in the combined Kucera-Francis corpus and the Time Magazine 1963 corpus were found. One occurrence was added to every word, so that words which did not occur in the corpus were given a value of 1, words that occurred once were given a value of 2, and so on. The total number of occurrences of these target words in the two corpora was 153,329, which when adjusted by 1 was 153,604. Each raw frequency was normalized based on the total (2,928 and 153,604), and a log base 10 ratio was formed between the two values. Words were sorted by their log ratio so that the words least likely to occur in normal text are shown first. Only words with a ratio greater than 0 (i.e., words that occurred in the annotations more frequently than would be expected; a total of 179 words) were shown. Log ratio p as the value in $1:(10^p)$ representing how much more often the word occurred than would have been expected by chance, where a value of 3 would mean 1:1000, a value of 2 would mean 1:100, and so on.

Word	Mentions	Log (Ratio)			
IED	139	3.86	cordon	4	1.62
VBIED	29	3.18	terrain	8	1.58
sniper	104	3.13	location	60	1.55
RPG	19	3.00	wooded	5	1.52
overwatch	8	2.62	obstructed	3	1.50
EFP	7	2.56	smuggling	4	1.48
triggerman	11	2.46	enemy	71	1.47
choke/chokepoint	32	2.45	insurgents	7	1.45
hilltop	5	2.42	elevated	6	1.42
spotter	9	2.37	marker	3	1.42
ambush	70	2.33	observation	15	1.40
PBIED	4	2.32	vest	3	1.35
dismounts	3	2.20	site	37	1.33
exfil	3	2.20	hidden	33	1.32
smallarms	3	2.20	rigged	4	1.32
SVIED	3	2.20	visibility	3	1.29
cache	8	2.15	grenade	4	1.28
rumble	8	2.02	route	26	1.25
vegetation	8	2.02	aiming	3	1.24
lookout	7	1.96	bulky	3	1.24
conceal	35	1.88	trigger	7	1.24
alleys	4	1.84	mortar	10	1.23
convoy	11	1.72	suicide	11	1.22
locals	4	1.72	patrol	9	1.21
intersection	20	1.70	dense	3	1.20
explosive	25	1.69	multiple	12	1.20
maneuver	10	1.68	tires	5	1.16
booby	4	1.62	bridge	40	1.16
			possible	109	1.13

potential	22	1.13	weapon	13	0.62
crossing	19	1.12	parked	3	0.62
detect	3	1.12	ground	18	0.61
pose	3	1.12	danger	7	0.59
pot	6	1.12	turns	3	0.54
ridge	4	1.12	watch	11	0.54
threat	21	1.12	area	42	0.54
roof	14	1.03	good	60	0.54
attack	43	1.03	looks	6	0.53
observe/observer	12	1.03	busy	4	0.50
buried	5	1.00	friendly	5	0.50
building	41	1.00	excellent	4	0.48
escape	15	0.99	hill	8	0.48
position	50	0.98	complex	6	0.48
trap	7	0.96	tree	10	0.47
cover	18	0.94	guy	3	0.46
pit	3	0.94	narrow	4	0.46
treat	6	0.94	bombs	3	0.45
vulnerable	3	0.94	conversation	3	0.45
vehicle	14	0.89	walking	3	0.44
bomber	7	0.87	ideal	4	0.44
dirt	6	0.86	avoid	4	0.42
caution	3	0.84	coalition	3	0.42
contain	6	0.84	advantage	4	0.40
traffic	11	0.81	indicate	4	0.40
road	38	0.80	hit	7	0.39
target	10	0.78	stream	3	0.38
due	17	0.75	high	30	0.38
offer	17	0.74	small	28	0.38
curve	5	0.74	market	13	0.37
team	14	0.73	command	5	0.37
risk	7	0.73	forward	6	0.35
entering	3	0.72	deep	6	0.34
point	45	0.72	sit	3	0.32
structures	3	0.71	main	6	0.29
arms	25	0.70	move/movement	18	0.29
village	9	0.70	forces	10	0.29
likely	16	0.70	easy/easily	9	0.27
fire	26	0.70	natural	6	0.27
contact	7	0.69	direct	5	0.27
access	3	0.68	open	13	0.27
bomb	5	0.68	fields	3	0.26
spot	7	0.68	soldier	6	0.25
allow	9	0.67	view	7	0.24
truck	7	0.67	place	29	0.24
abandoned	3	0.67	cars	5	0.23
wire	5	0.66	town	9	0.23
urban	4	0.65	mass	4	0.23
windows	5	0.63	crowd	3	0.21
exposed	3	0.63	side	17	0.21
slow	6	0.62	lack	4	0.20

materials	3	0.19
pass	3	0.19
provide	9	0.18
wall	8	0.17
distance	3	0.15
making	8	0.14
cause	4	0.13
quickly	3	0.13
security	4	0.12
activity	3	0.11
corner	3	0.11
break	3	0.10
along	10	0.08
difficult	4	0.08
attention	4	0.04
river	4	0.03
population	4	0.03
hard	6	0.02
large	8	0.01
inside	4	0.00

Appendix L

Major Comments from Interviews – Phase II

- Get reports to come to areas where sniper activity is known to be...we keep eyes out on buildings as far as we can see to look for suspicious movements...we see people on top of roofs carrying things around, we don't know what they have.
- Intel and social networks within Iraq (i.e., rehabilitated insurgents, locals, suspect family members)...90% of the people we locked up was because of those things.
- Usually a driver can pick out a person [in a crowd] with a weapon faster, so I have him look in the crowd for people with weapons and let me know.
- 30% of the time, the stuff that pays off [resulting in catching/stopping a threat] comes from talking to people.
- Information is a big thing. If you cordon off the area and start talking to people, somebody out there knows exactly what is going on.
- Do not dismiss what the Soldiers see. It might look normal to me, but if it looks funny to him, we need to check it out. If we are not supposed to check it out or we do not have the equipment to check it out at least take steps to report it.
- We know if it rained the day before we are going to really focus on mounds of mud on the side of the road. When it's dry and the mud is hard we can see it from a distance, but it's easier to conceal it after it rains.
- Look for disturbed dirt; anything attached to the side of the barrier; dead dogs that will have bombs in them...most detection is done with equipment. If you're on the ground walking, look for cords in the road.

Soldiers also reported facing challenges when sorting and filtering information and when trying to interpret the cues they observe:

- When you first get there, everybody is a threat...all we have to go on is what the populace says. When you go into a town you paint a mental picture and that helps you narrow things down. You might be off as far as the cells go, but at least you have more than you did when you go there.
- Once the cues (the visual or the vocal cues) become so many that you can't follow them all, then you're in a dangerous spot. It just becomes overwhelming.
- My worst fear is when we cross a bridge, noticing where things are because if you get in a situation, especially in the middle, you can't go forward or back.
- So many vehicles on route that it's hard to see the IEDs. There are trucks everywhere and it's hard to see through the traffic. Trucks are on either side of you and you don't know if one is carrying a weapon or IED.
- Time we get called out at midnight or 3:00 in the morning, it's harder to see things even though we have [night vision goggles] NVGs; we still have less chance of seeing what's going on around us than during the day...biggest challenge is visibility.
- You can't follow everything. You could speculate that's potential for stress...you have to psychologically numb yourself and just accept the fact that there could be a sniper in any one of these windows or any of these carts on the side of the road could blow up. What can you do? You can't stop every five feet and search every person or every

vehicle or every satchel on the side of the road or look in every window before you proceed forward. It would take you all day to get three blocks down the street.

- More difficult to detect threats in the city because of all the trash and debris...it's a little easier in the desert because it's just a lot of dirt and it's easier to tell where something has been dug up or where something is different.

These statements indicate that the ability to detect threat cues and then to evaluate and separate relevant from irrelevant information is vital to assessing the operational environment and to making accurate responses to valid threats. Similarly, Soldiers discussed the importance of spotting trends and noticing changes in the environment. Some examples include:

- You're in an area enough you start to recognize the norms and then you can pick out what's not normal activity (like woman looking you in the eye, walking straight at you).
- One of the benefits of going out every day is you can tell when the populace isn't acting the way they normally did. They never wanted to talk to us; but they knew when something was going down. They didn't want to be around us those days.
- After six months or so we started realizing what kind of triggers they used and what areas they liked hitting us in...we got a lot better at detecting it way ahead of the game.
- Training on knowing how the enemy fights in *your* area (e.g., IEDs in soda cans; people on bicycles)...if over the last month all of the IEDs have come out of Coke cans, they should be getting that info. Maybe in training, have the "insurgents" fight a certain way and then switch it and see if they react to it. You have a couple of rock piles and after a while, all they look for is rock piles. If you set up a rock pile with nothing in it and when they all focus their attention on that have an explosion somewhere else and see how they handle it.
- Patrols...they see a red marker like a piece of paint on the telephone pole. Couple of days later, another unit sees the same thing. Same place, same type of marker. So we flew around it, maybe helicopter attacked it, blew it up.
- We'd talk with people and know that there was a high probability of stuff going on in that area...don't know how much that enabled us to change our plans.
- Study current trends, then see how [adversary] can change them a bit to make them different. E.g., we were finding IEDs, generally they made them look like pieces of broken concrete. At first, there would be broken pieces of concrete on the side of the road and we'd find them. So then, they'd have them 3 meters off the road, but they made them look like dirt or mud. They used similar tactics, but they changed the color of the IED to make it look like mud.
- Good at predictive analysis; studying current trends and asking what-if questions. This is really important if you've been successful at identifying threats because the threats are going to change now. You have to take the bits of intel that are out there and put all the pieces together like a puzzle to figure out what they're going to do next.
- You go down the same routes every day, you start to memorize the environment and recognize changes.

Appendix M

Exercise Descriptions – Phase III

The following is a detailed description of the exercises and what constructs intended to be measured with each exercise.

Method

Participants

Four U.S. Army Soldiers took part in the preliminary experiment (1 NCO, E-5; 3 officers, 2LT to MAJ). All Soldiers were male, with a mean age of 33 (range 24-45), and a mean time in service of 63 months (range 12-108 months).

Materials

Demographic and Threat Questionnaires. The demographic questions (Appendix B) and threat questionnaire (Appendix C) were the same as used in Phases I and II.

Imagery Analysis. Ten images were selected to cover a range of potential threat situations, such as topographical maps, aerial imagery, and ground-based photos. The photos used in Phase III included those used in Phase II and included new DoD-produced photos retrieved from www.DefenseImagery.mil, www.Flickr.com, and www.defense.gov. All photos were cleared for public release and unlimited usage.

Interview protocol. The interviews in this phase focused on gathering information about the causal reasoning used to make threat detection choices during the computer exercises. Soldiers viewed a set of pictures (Appendix N) and chose several that reminded them of their previous threat detection experiences (training and/or operational). Soldiers described the threat-related events that might occur and discussed possible threat scenarios. Soldiers also explained why they were concerned about particular threats, described threat indicators, and discussed how the situation might play out if the threat were real.

Procedure

This phase involved two main parts: a computer-controlled exercise, and a semi-structured interview. At the start of each session, Soldiers were provided with a description of the exercises. They learned that the purpose of the project was to capture their threat detection experiences and identify common threat detection situations, indicators, and challenges in the OE. Soldiers then completed the computer exercises at their own pace. They could ask clarification questions during the session.

Following the demographic questions, Soldiers completed three computerized exercises that attempted to measure attention, search, reasoning, and prioritization strategies for threat detection. The first paradigm implemented a causal reasoning exercise, the second implemented

a resource-limited search process, and the third an attention-monitoring process. The computerized exercise typically took place first, and lasted between 30 and 45 minutes.

After the computer exercises, Soldiers were interviewed about their threat detection experiences. The interviews lasted approximately one hour. At the end of the session, Soldiers could ask questions and provide feedback about the experiment materials and direction for the project. Soldiers were debriefed and given contact information for mental health assistance that they could use if discussion of their experiences brought up any negative feelings or memories.

Dynamic Threat Monitoring - Single task. A distinct aspect of threat detection is the ability to maintain vigilance over a visual scene. It was not suspected that vigilance strategies would distribute search uniformly around the visual environment, but rather focus search on a few highly likely threat locations. Though eye movements were not monitored explicitly, this test assessed visual search by requiring the Soldier to search an image occluded by noise (semi-transparent grey circles) for a target (unfilled orange circle) which could appear in either threat-consistent or threat-inconsistent areas (Figure 10). This design is akin to studies of covert attention shifts, in that a particular piece of prior information can influence how a visual scene is processed, but the cue here is implicit, and depends on the Soldier's experience with such threats.



Figure M.1. Screenshot of the Dynamic Threat Monitoring, Single-task.

In this exercise, Soldiers monitored each image for an orange outlined circle the same size as the dynamic grey circle noise. When the circle appeared, the Soldiers would click the

screen with the mouse to signal a detection, and then click on the location to identify the target. The computer displayed each of the ten images for one minute, presenting seven threat-relevant targets and three threat-irrelevant targets.

Dynamic Threat Monitoring - Dual-task. During half the trials, a secondary light panel was also present requiring Soldiers to monitor both the photo and the light panel for a specific pattern and respond similarly to the orange target (Figure 11). Soldiers' attention resources are often split between different tasks or sources of information in the OE. This dual-task allowed an assessment of the limitations on dynamic threat monitoring.



Figure M.. Screenshot of the Dynamic Threat Monitoring, Dual-task.

Threat Search (Prioritization). The threat search exercise was essentially a modified version of the imagery analysis exercise performed during Phase II. The exercise was modified to provide a more reliable method for identifying the high priority threats. Soldiers viewed an image, and read instructions informing them that they had at their disposal a special “microwave scope” that could detect explosive material from a distance (Figure 12). We informed them that this scope was not perfect, so that searching in a particular location would not guarantee they would find a target that was present. The scope had a limited number of uses, which required Soldiers to search efficiently. This search method placed a de facto cost on search because Soldiers could perform only a limited number of searches. When Soldiers clicked on a location in an image, a transparent green scope appeared briefly at that location and, if present, revealed

pre-specified targets within the scope. These red targets only appeared when Soldiers clicked on that location with the scope.

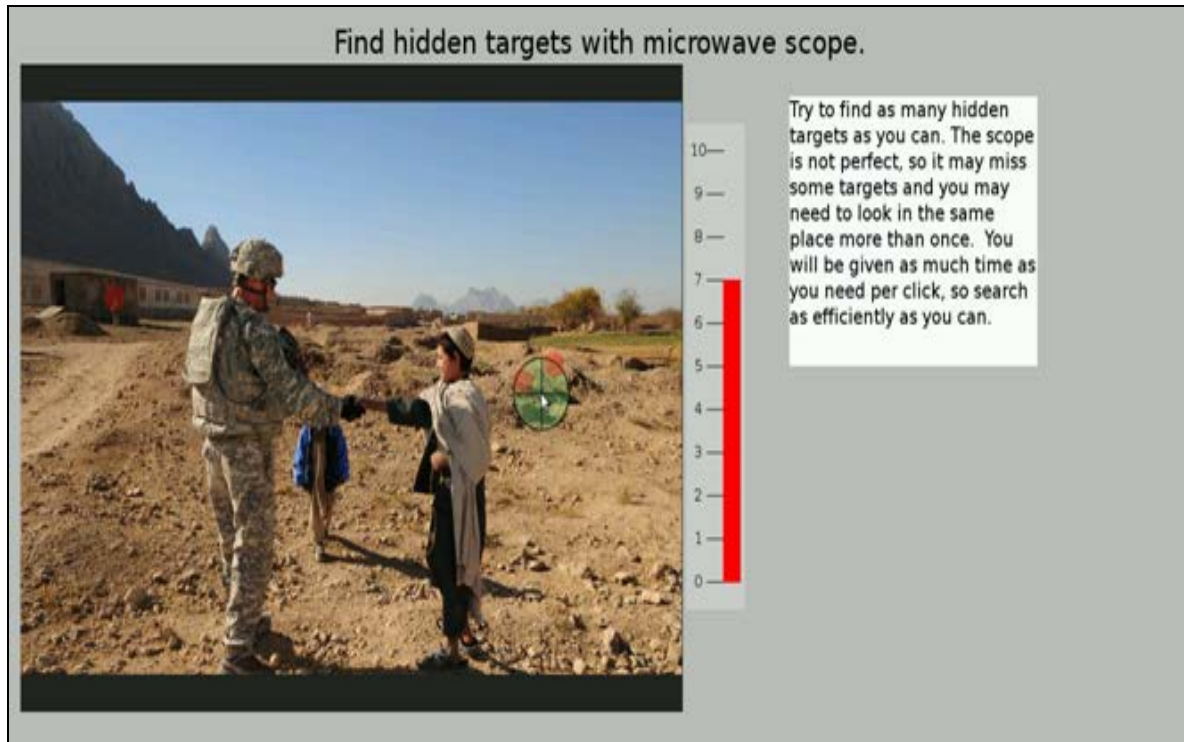


Figure M.3. Screenshot of the Threat Search/Prioritization Exercise.

The threat search exercise consisted of timed and untimed conditions. In the untimed condition, Soldiers had as much time as they needed to search for threats, though they could only make 10 clicks on the image. Upon each click, a red vertical usage meter decremented by one unit until they used all 10. In the timed condition, the usage meter got smaller continuously with time, and on each click, the meter decremented to the next lower even number. Soldiers could make up to 10 clicks per image in the timed condition, if they were identifying targets at a rate greater than one per second.

Between 15 and 30 hidden target locations were selected per image. For images used during Phase II, the locations were selected based on the previously annotated locations. The remaining images, were selected based on the themes identified in Phase II. However, the source of the threat targets was not critical in this stage of the research because the interest was not in the efficiency of search strategies and the types of targets Soldiers focused on rather than how many of the targets the Soldiers found. Fifty-eight images were used, with half randomly selected for the timed condition, and half selected for untimed condition.

Causal Reasoning. The previous research suggested that a major component of threat detection involves causal reasoning. To detect threats, Soldiers do not simply search for cues related to threat, they must also undergo a reasoning process about why certain cues are present, and what makes locations attractive places for an enemy to emplace an IED or execute an attack.

For example, simple cues to a potential threat might be a location that had been bombed previously, or a pile of rubble next to a road. Deeper reasoning might consider how the type of triggering mechanism currently used for IEDs (victim-activated, wire, or wireless) changes the needs of the enemy (how far they need to hide from the attack location). Also implicit in the hiding process are issues like easy avenues of escape, and ability to blend with the local populace. Finally, the goal of using IEDs, and similar, attacks must be considered: the casualties or equipment damage that an IED may produce is often secondary, and other factors drive the placement, such as the ability to prevent non-combatant harm, and the ability to record and publicize the attack.

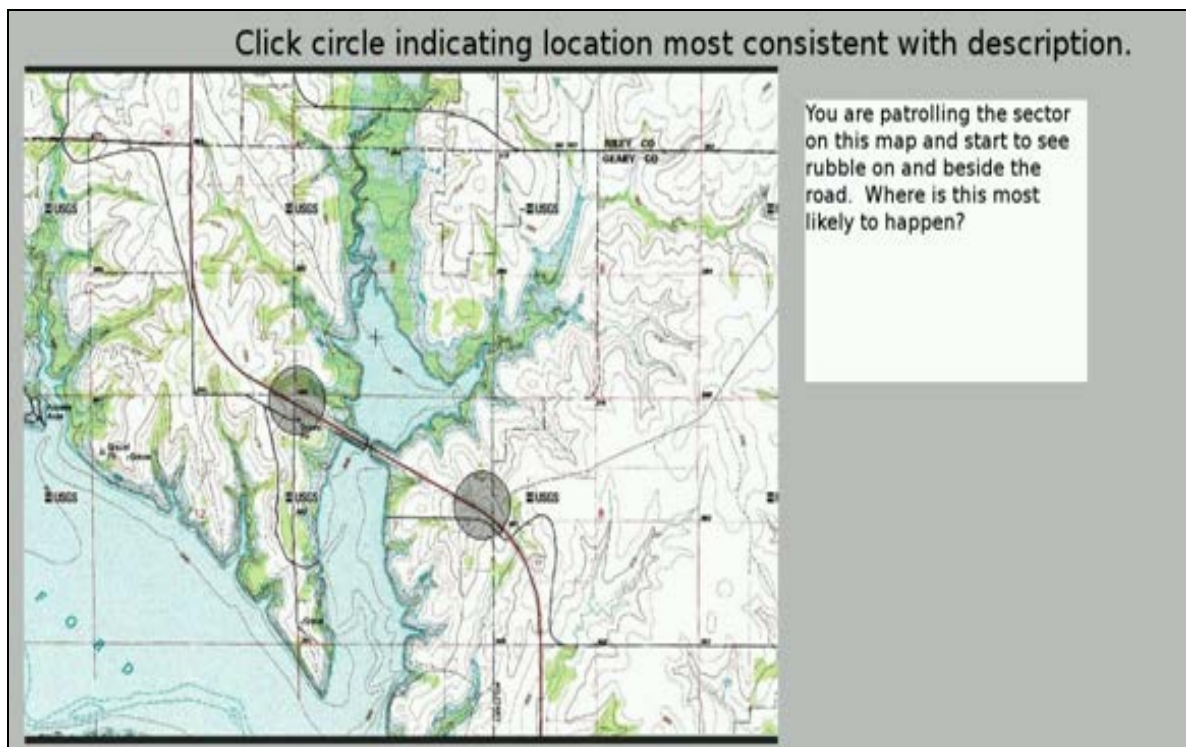


Figure M.4. Screenshot of the Causal Reasoning Exercise.

A forced-choice method was developed as a platform to assess causal reasoning. We selected two locations on each image and posed a question that required selecting one of the two locations (Figure 13). Soldiers responded to the question by clicking on one of the grey circles. Though there was no objectively correct response to any of the questions, the options were designed so that choosing one option would imply some deeper level of reasoning than choosing the other.

Appendix N

Interview Photos – Phase III

